МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Конспект лекцій з дисципліни
«Інформаційне забезпечення фінансово-економічної безпеки»
для студентів освітньо-кваліфікаційного рівня **«магістр»,**
спеціальності – **073 «Менеджмент»,**
спеціалізація **«Управління фінансово-економічною безпекою»**

Обговорено і рекомендовано
на засіданні кафедри
фінансово-економічної
безпеки
Протокол № 11
від *«3» травня 2017 р.*

ЧЕРНІГІВ ЧНТУ 2017

Інформаційне забезпечення фінансово-економічної безпеки. Конспект лекцій з дисципліни «Інформаційне забезпечення фінансово-економічної безпеки», для студентів освітньо-кваліфікаційного рівня «магістр», спеціальності – 073 «Менеджмент», спеціалізація «Управління фінансово-економічною безпекою» / Укл. Жарій Я.В., Садчикова І.В.– Чернігів: ЧНТУ, 2017. – 159 с.

Укладачі: Жарій Ядвіга Вікентіївна, кандидат технічних наук, доцент
Садчикова Ірина Володимирівна, кандидат економічних наук, доцент

Відповідальний за випуск: Лапінський І.Е., завідувач кафедри фінансово-економічної безпеки, кандидат економічних наук, доцент

Рецензент: Лисенко І.В., кандидат економічних наук, доцент кафедри фінансово-економічної безпеки Чернігівського національного технологічного університету

ЗМІСТ

ВСТУП

В умовах глобальної інформатизації всіх сфер життя практично неможливо приймати ефективні рішення без їх всебічного і об'єктивного інформаційного забезпечення. Ризик використання неповної або необ'єктивної інформації в управлінських рішеннях сьогодні істотно впливає на успіх як конкретної комерційної операції, так і в цілому підприємницької діяльності. В умовах обмежених можливостей отримання суб'єктами вітчизняного підприємництва необхідної їм інформації через відсутність певних правових норм, методи інформаційно-аналітичної роботи виступають основним засобом формування інформаційних ресурсів усіх видів підприємств.

Усе це має безпосереднє відношення до діяльності співробітників структур служб безпеки підприємств. За таких обставин сучасний фахівець з питань безпеки підприємництва повинен вміти грамотно здійснювати пошук та збір інформації необхідної для його діяльності та діяльності його підприємства, оцінювати та використовувати її. Виходячи з цього велике значення має володіння відповідними фахівцями основними формами, методами та досвідом формування інформаційних ресурсів підприємства та основ їх використання у інтересах захисту безпеки підприємств.

Поширення комп'ютерних систем, об'єднання їх у комунікаційні мережі підсилює можливості електронного проникнення в них. Проблема комп'ютерної злочинності у всіх країнах миру, незалежно від їхнього географічного положення, викликає необхідність залучення все більшої уваги й сил громадськості для організації боротьби з даним видом злочинів. Особливо широкий розмах одержали злочини в автоматизованих банківських системах і в електронній комерції. За закордонним даними, втрати в банках у результаті комп'ютерних злочинів щорічно становлять багато мільярдів доларів. Хоча рівень впровадження новітніх інформаційних технологій у практику в Україні не настільки значний, комп'ютерні злочини з кожним днем дають про себе знати усе більше й більше, а захист держави й суспільства від них перетворилася в серйозну проблему.

Кожний збій роботи комп'ютерної мережі це не тільки «моральний» збиток для працівників підприємства й мережних адміністраторів. По мірі розвитку технологій електронних платежів, «безпаперового» документообігу й інших інформаційних технологій, серйозний збій локальних мереж може просто паралізувати роботу цілих корпорацій і банків, що приводить до відчутних матеріальних втрат. Не випадково, що захист даних у комп'ютерних мережах стає однієї із самих гострих проблем на сьогоднішній день.

Мета викладання нормативної навчальної дисципліни «Інформаційне забезпечення фінансово-економічної безпеки» циклу професійної підготовки – опанування методикою моніторингу та аналізу загроз фінансовій та економічній діяльності підприємства і побудові систем забезпечення безпеки на основі сучасних ІС.

Основними завданнями вивчення дисципліни є:

− отримання знань характеристик реальних та потенційних загроз діяльності підприємства;

– вміння будувати систему моніторингу та аналізу надзвичайних подій;

– вміння організовувати систему збору, поширення та зберігання інформації;

– отримання навичок розробки проектів положень, наказів та інструкцій, що регламентують діяльність підрозділу фінансово-економічної безпеки.

Студент повинен знати:

– характеристики зовнішнього і внутрішнього середовища підприємства;

– методи і засоби пошуку, збору та оцінки інформації ;

– законодавчі та нормативні акти, що регламентують діяльність підрозділу фінансово-економічної безпеки;

– аналітичне забезпечення системи управління фінансово-економічною безпекою;

Студент повинен вміти:

– визначати фактори, що впливають на фінансово-економічну безпеку підприємства;

– розробляти проекти положень, наказів та інструкцій, що регламентують діяльність підрозділу фінансово-економічної безпеки;

– розробляти системи фінансово-економічної безпеки.

Тема 1. *Концептуальні засади інформаційно-аналітичного забезпечення безпеки підприємства*

План:

1.1 Базові поняття інформаційного забезпечення фінансово-економічної безпеки підприємства.

1.2 Методологія інформаційного забезпечення фінансово-економічної безпеки діяльності підприємства.

1.3 Політика інформаційної безпеки.

1.4 Критерії безпеки інформаційної безпеки

1.1 Базові поняття інформаційно-аналітичного забезпечення безпеки підприємства.

Сучасне суспільство називається інформаційним. Широкий розвиток засобів обчислювальної техніки й зв'язку дозволило збирати, зберігати, обробляти й передавати інформацію в таких обсягах і з такою оперативністю, які були немислимі раніше. Завдяки новим інформаційним технологіям виробнича й невиробнича діяльність людини, його повсякденна сфера спілкування безмежно розширюються за рахунок залучення досвіду, знань і духовних цінностей, вироблених світовою цивілізацією, і сама економіка все в меншому ступені характеризується як виробництво матеріальних благ і все в більшої як поширення інформаційних продуктів і послуг.

Сучасний етап інформатизації пов'язаний з використанням електронно-обчислювальної техніки, систем телекомунікацій, створення мереж ЕОМ. Зростає потреба в розробці й застосуванні ефективних рішень у сфері інформаційної індустрії. Вона займається виробництвом технічних і програмних засобів, інформаційних технологій для одержання нових знань.

На певному етапі розвитку інформаційної індустрії народжується інформаційне суспільство, у якому більшість працюючих зайнята виробництвом, зберіганням, переробкою й реалізацією інформації, тобто творчою працею, спрямованою на розвиток інтелекту й одержання знань. Створюється єдине, не розділене національними кордонами інформаційне співтовариство людей.

Формування інформаційного суспільства опирається на новітні інформаційні, телекомунікаційні технології й технології зв'язку. Саме нові технології привели до бурхливого поширення глобальних інформаційних мереж, що відкривають принципово нові можливості міжнародного інформаційного обміну. Формування інформаційного суспільства концептуально й практично означає формування світового інформаційного простору.

Інформаційний простір – сфера людської діяльності, що пов'язана зі створенням, перетворенням і споживанням інформації й включає в себе:

- індивідуальну й суспільну свідомість;
- інформаційні ресурси, тобто інформаційну інфраструктуру (комплекс

організаційних структур, технічних коштів, програмного й іншого забезпечення для формування, зберігання, обробки й передачі інформації), а також безпосередньо саму інформацію і її потоки.

Інформаційна війна – це інформаційне протиборство з метою завдання збитків важливим структурам супротивника, підриву його політичної й соціальної систем, а також дестабілізації суспільства й держави супротивника.

Інформаційне протиборство – форма міждержавного суперництва, реалізована за допомогою надання інформаційного впливу на системи керування інших держав і їхніх збройних сил, а також на політичне й військове керівництво й суспільство в цілому, інформаційну інфраструктуру й засоби масової інформації цих держав для досягнення вигідних для себе цілей при одночасному захисті від аналогічних дій від свого інформаційного простору.

Інформаційна злочинність – проведення інформаційних впливів на інформаційний простір або будь-який його елемент у протиправних цілях. Як її приватний вид може розглядатися інформаційний тероризм, тобто діяльність, проведена в політичних цілях.

Інформаційний вплив – акт застосування інформаційної зброї.

Інформаційна зброя – комплекс технічних і інших коштів, методів і технологій, призначених для:

- установлення контролю над інформаційними ресурсами потенційного супротивника;
- втручання в роботу його систем керування й інформаційних мереж, систем зв'язку й т.п. з метою порушення їхньої працездатності, аж до повного виведення з ладу, вилучення, перекручування даних, що втримуються в них, або спрямованого введення спеціальної інформації;
- поширення вигідної інформації й дезінформації в системі формування суспільної думки й прийняття рішень;
- вплив на свідомість і психіку політичного й військового керівництва, особового складу збройних сил, спецслужб і населення конфронтуючої держави, використовуваних для досягнення переваги над супротивником або ослаблення проведених їм інформаційних впливів.

Під **погрозою безпеки інформації** розуміються події або дії, які можуть привести до перекручування, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних коштів.

У своїх протиправних діях, спрямованих на оволодіння чужими секретами, зломщики прагнуть знайти такі джерела конфіденційної інформації, які б давали їм найбільш достовірну інформацію в максимальних обсягах з мінімальними витратами на її одержання. За допомогою різного виду вивертів і безлічі прийомів і засобів підбираються шляхи й підходи до таких джерел. У цьому випадку під джерелом інформації розуміється матеріальний об'єкт, який містить певні відомості, що представляють конкретний інтерес для зловмисників або конкурентів.

Інформаційна безпека включає:

– стан захищеності інформаційного простору, що забезпечує його формування й розвиток в інтересах громадян, організацій і держави;

– стан інфраструктури, при якому інформація використовується строго по призначенню й не робить негативного впливу на систему при її використанні;

– стан інформації, при якому виключається або істотно утруднюється порушення таких її властивостей, як конфіденційність, цілісність і доступність;

– економічну складову (структури керування в економічній сфері, включаючи системи збору, нагромадження й обробки інформації в інтересах керування виробничими структурами, системи загальекономічного аналізу й прогнозування господарського розвитку, системи керування й координації в промисловості й на транспорті, системи керування енергосистемами, централізованого постачання, системи ухвалення рішення й координації дій у надзвичайних ситуаціях, інформаційні й телекомунікаційні системи);

– фінансову складову (інформаційні мережі й бази даних банків і банківських об'єднань, системи фінансового обміну й фінансових розрахунків).

Виходячи з вищевикладеного, у найбільш загальному виді інформаційна безпека може бути визначена як неможливість нанесення шкоди властивостям об'єкта безпеки, що обумовлюється інформацією й інформаційною інфраструктурою (рис. 1.1).

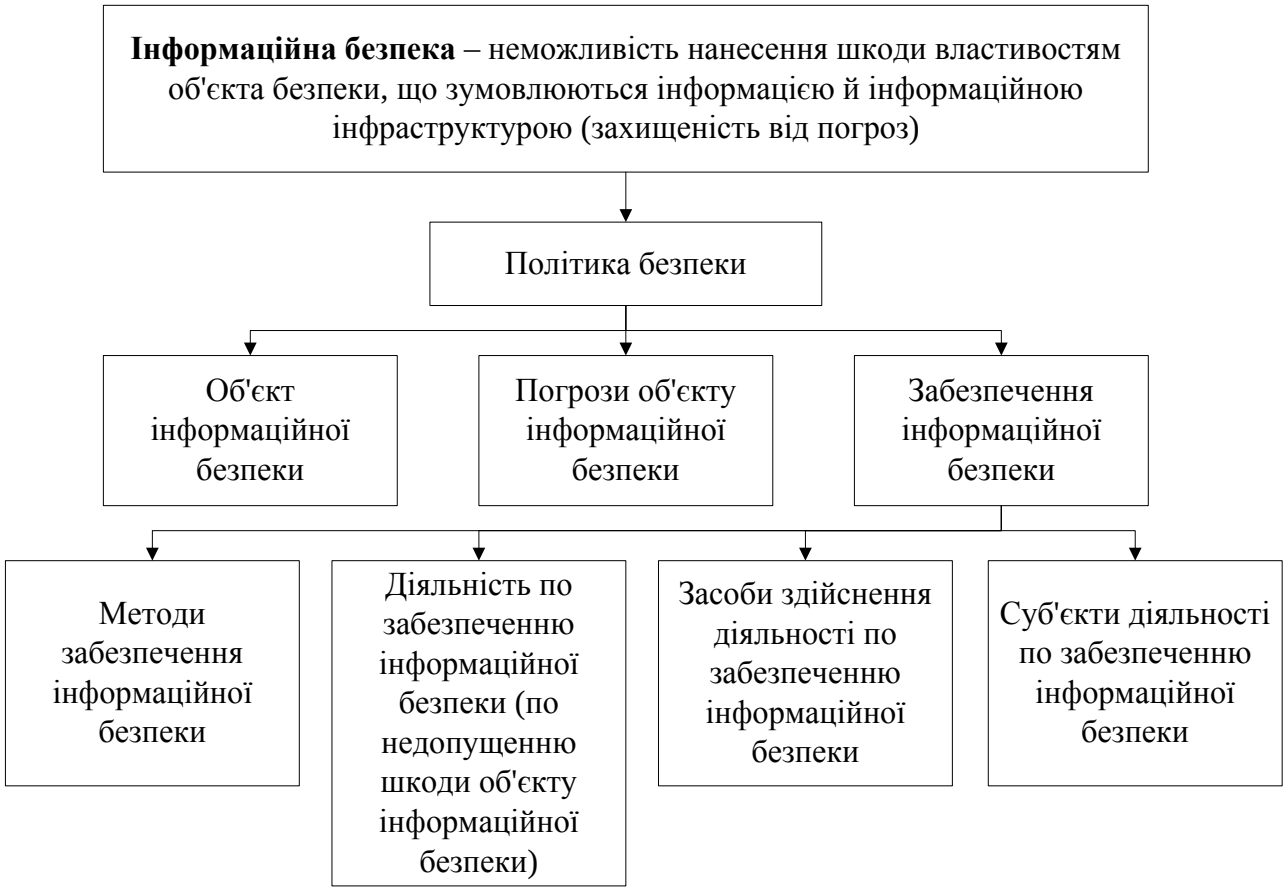

Рис. 1.1. Структура поняття «Інформаційна безпека»

Поняття інформаційної безпеки у вузькому змісті цього слова має на увазі:

- надійність роботи комп'ютера;
- схоронність важливих даних;
- захист інформації від внесення в неї змін з особами; що не мають повноважень на це;
- збереження таємниці листування в електронному зв'язку.

Безпека проявляється як неможливість нанесення шкоди функціонуванню й властивостям об'єкта або його структурним складовим.

Об'єктом інформаційної безпеки може бути комерційне підприємство. Тоді визначення «інформаційної безпеки» буде укладатися в захищеності інтересів власника даного підприємства, що задовольняються за допомогою інформації, або пов'язаних із захистом від несанкціонованого доступу тих відомостей, які представляються власникові досить важливими. Інтереси проявляються через об'єкти, здатні служити для їхнього задоволення, і дії, що вживаються для володіння цими об'єктами. Відповідно інтереси як об'єкт безпеки можуть бути представлені сукупністю інформації, здатної задовольняти інтерес власника і його дій, спрямованих на оволодіння інформацією або приховання інформації. Ці складові об'єкта інформаційної безпеки й захищаються від зовнішніх і внутрішніх погроз.

До об'єктів інформаційної безпеки на підприємстві відносять:

- інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, і конфіденційну інформацію, представлену у вигляді інформаційних масивів і баз даних;
- засоби й системи інформатизації – засоби обчислювальної й організаційної техніки, мережі й системи, загальносистемне й прикладне програмне забезпечення, автоматизовані системи керування підприємствами, системи зв'язку й передачі даних, технічні засоби збору, реєстрації, передачі, обробки й відображення інформації, а також їх інформативні фізичні поля.

При здійсненні комерційної діяльності виникає інформація, обізнаність з якою іншими учасниками ринку може істотно знизити прибутковість цієї діяльності. У діяльності держави породжується інформація, розкриття якої може знизити ефективність проведеної політики. Подібна інформація закривається, і встановлюваний режим її використання покликаний попередити можливість несанкціонованого ознайомлення з нею. У цьому випадку об'єктом безпеки виступає режим доступу до інформації, а інформаційна безпека укладається в неможливості порушення цього режиму. Прикладом можуть служити інформаційно-телекомунікаційні системи й засоби зв'язку, призначені для обробки й передачі відомостей, що становлять державну таємницю. Основним об'єктом безпеки в них є режим доступу до секретної інформації. Інформаційна безпека таких систем укладається в захищеності цієї інформації від несанкціонованого доступу, знищення, зміни й інших дій. Система забезпечення безпеки інформації включає підсистеми:

- комп'ютерна безпека;

– безпека даних;
– безпечне програмне забезпечення;
– безпека комунікацій.

Комп'ютерна безпека забезпечується комплексом технологічних і адміністративних заходів, застосовуваних відносно апаратних засобів комп'ютера з метою забезпечення доступності, цілісності й конфіденційності, пов'язаних з ним ресурсів.

Безпека даних досягається захистом даних від неавторизованих, випадкових, навмисних або виниклих по недбалості модифікацій, руйнувань або розголошень інформації.

Безпечне програмне забезпечення являє собою загальносистемні й прикладні програми й кошти, що здійснюють безпечну обробку даних і безпечно, що використовують ресурси, системи.

Безпека комунікацій забезпечується вживанням заходів по запобіганню надання неавторизованим особам інформації, що може бути видана системою у відповідь на телекомунікаційний запит.

Захист інформації (ЗІ) – комплекс заходів, спрямованих на забезпечення найважливіших аспектів інформаційної безпеки: цілісності, доступності й, якщо потрібно, конфіденційності інформації й ресурсів, використовуваних для уведення, зберігання, обробки й передачі даних.

Основні предметні напрямки ЗІ – охорона державних, комерційних, службових, банківської таємниць, персональних даних і інтелектуальної власності.

Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства й держави від внутрішніх і зовнішніх погроз.

Система захисту інформації представляє організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх погроз

З позицій системного підходу до захисту інформації пред'являються певні вимоги:

– забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні й реалізації найбільш раціональних методів, способів і шляхів удосконалення й розвитку системи захисту, безперервному контролі її стану, виявлення її вузьких і слабких місць і протиправних дій;

– безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах економічної системи й на всіх етапах технологічного циклу обробки інформації;

– планування безпеки інформації здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції;

– захисту підлягають конкретні дані, об'єктивно підмети охороні,

втрата яких може заподіяти організації певний збиток;

– методи й засоби захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних секретів;

– ефективність захисту інформації означає, що витрати на її здійснення не повинні бути більше можливих втрат від реалізації інформаційних погроз;

– чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;

– надання користувачеві мінімальних повноважень, необхідних йому для виконання дорученої роботи;

– відомість до мінімуму числа загальних для декількох користувачів засобів захисту;

– облік випадків і спроб несанкціонованого доступу до конфіденційної інформації; забезпечення ступеня конфіденційної інформації;

– забезпечення контролю цілісності засобів захисту й негайне реагування на їхній вихід з ладу.

Система захисту інформації, як будь-яка система, повинна мати певні види власного забезпечення, опираючись на які вона буде виконувати свою цільову функцію. З урахуванням цього система захисту інформації може мати:

– правове забезпечення. Сюди входять нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери дії;

– організаційне забезпечення. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями, такими як: служба безпеки, служба режиму, служба захисту інформації технічними коштами й ін.;

– апаратне забезпечення. Передбачається широке використання технічних засобів, як для захисту інформації, так і для забезпечення діяльності безпосередньо системи захисту інформації;

– інформаційне забезпечення. Воно містить у собі документовані відомості (показники, файли), що лежать в основі рішення завдань, що забезпечують функціонування системи. Сюди можуть входити як показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;

– програмне забезпечення. До нього ставляться антивірусні програми, а також програми (або частини програм регулярного застосування), що реалізують контрольні функції при рішенні облікових, статистичних, фінансових, кредитних і інших завдань;

– математичне забезпечення. Припускає використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;

– лінгвістичне забезпечення. Сукупність спеціальних язикових засобів спілкування фахівців і користувачів у сфері захисту інформації;

– нормативно-методичне забезпечення. Сюди входять норми й регламенти діяльності органів, служб, засобів, що реалізують функції захисту

інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації;

– ергономічне забезпечення. Сукупність засобів, що забезпечують зручності роботи користувачів апаратних засобів захисту інформації.

У ринкових умовах господарювання підприємство, як відкрита система, функціонує у складному зовнішньому середовищі, що характеризується нестабільністю та постійною динамікою. Таке середовище змушує керівництво швидко адаптуватися до нових умов, потребує знання законів розвитку та пошуку шляхів виживання в ринковій економіці, врахування чинників невизначеності та нестійкості економічного середовища.

Найважливішими факторами, що впливають на економічну безпеку підприємства, є ступінь досконалості законодавчої бази, рівень оподаткування, доступ на світові ринки збуту, інвестиційна привабливість регіону, держави. Насамперед, економічна-безпека підприємства залежить від економічної безпеки держави, регіону, адже ґрунтується на їхньому фінансовому, сировинному та виробничому потенціалі, перспективах розвитку. Наявність багаторівневої концепції економічної безпеки господарюючих суб'єктів усіх рівнів дає можливість забезпечити передбачуваність зовнішніх загроз підприємствам.

Економічній безпеці підприємства властивий подвійний характер: з одного боку, вона забезпечує можливість власного функціонування, з іншого – є частиною (елементом) економічної безпеки системи вищого рівня і суб'єктом, що забезпечує виконання функцій регіоном, державою. В перехідні періоди розвитку економіки домінуючими є дослідження макроекономічних аспектів економічної безпеки.

Поняття «економічна безпека» пройшло чимало переосмислень у зв'язку зі зміною умов зовнішнього середовища і з урахуванням факторів, які зумовлюють процеси управління. Вперше поняття «економічна безпека» почало застосовуватися на Заході у зв'язку зі зростанням проблеми обмеженості ресурсів та розпадом колоніальної системи, що призвело до порушення традиційних зв'язків між постачальниками ресурсів, життєво необхідних індустріальним суспільствам.

Сутність економічної безпеки підприємств полягає в забезпеченні поступального економічного розвитку суспільства з метою виробництва необхідних благ та послуг, що задовольняють індивідуальні та суспільні потреби. Раніше усі питання, пов'язані із забезпеченням безпеки покладалися на державні органи. Останнім часом спостерігається відтворення системи безпеки, в якій провідна роль відводиться державі.

На мікрорівні економічна безпека проявляється в забезпеченні нормальної і стабільної діяльності підприємства, попередженні витоку інформації.

Економічну безпеку підприємства можна трактувати, як:

– стан захищеності усіх систем підприємства при здійсненні господарської діяльності в певній ситуації;

– стан всіх ресурсів підприємства (капіталу, трудових ресурсів, інформації, технологій, техніки, прав) та підприємницьких здібностей, при якому можливе найефективніше їх використання для стабільного функціонування і динамічного науково-технічного та соціального розвитку, здатність запобігати або швидко нівелювати різні внутрішні та зовнішні загрози;

– сукупність організаційно-правових, режимно-охоронних, технічних, технологічних, економічних, фінансових, інформаційно-аналітичних та інших методів, спрямованих на усунення потенційних загроз та створення умов для забезпечення ефективного функціонування суб'єктів підприємницької діяльності відповідно до їхніх цілей та завдань;

– стан соціально-технічної системи підприємства, котрий дає змогу уникнути зовнішніх загроз і протистояти внутрішнім чинникам дезорганізації за допомогою наявних ресурсів, підприємницьких здібностей менеджерів, а також структурної організації та зв'язків менеджменту.

Головна мста управління економічною безпекою – забезпечення найефективнішого функціонування, найпродуктивнішої роботи операційної системи та економічного використання ресурсів, забезпечення певного рівня трудового життя персоналу та якості господарських процесів підприємства, а також постійного стимулювати нарощування наявного потенціалу та його стабільного розвитку.

Система заходів економічної безпеки підприємства може бути представлена наступними складовими:

– прогнозування можливих загроз економічної безпеки;

– організація діяльності з попередження можливих загроз (превентивні заходи);

– виявлення, аналіз і оцінка виниклих реальних загроз економічної безпеки;

– прийняття рішень та організація діяльності з реагування на виниклі загрози;

– постійне вдосконалення системи забезпечення економічної безпеки підприємництва.

Інформаційне забезпечення фінансово-економічної безпеки підприємництва (ІЗФЕБП) – це вид інформаційного забезпечення підприємницької діяльності шляхом добування, обробки і надання керівництву необхідної інформації. Необхідна при оцінці обстановки і прийняття рішення на відповідному рівні в інтересах розвитку підприємства.

Головна мета ІЗФЕБП – викриття на ранній стадії заходів безпосередньої підготовки певних ворожих сил з метою нанесення економічних збитків підприємству та забезпечення відповідних їм дій за допомогою добування необхідної інформації для планування, підготовки і проведення заходів задля недопущення можливих дій.

В основі ІАЗБП лежить інформаційно-аналітична діяльність.

Інформаційно-аналітична діяльність (ІАД) – це творчий процес в системі ІЗФЕБ різного рівня, який включає комплекс заходів, що організується

і проводиться СБ підприємства та їх структурними підрозділами з метою збору та обробки необхідних відомостей з ряду питань і на підставі проведеної роботи – розробки інформаційних (інформаційно-аналітичних) документів для керівництва.

Інформаційно-аналітична діяльність полягає в узагальненні одержаної інформації, що добувається в результаті проведення розвідувально-оперативної діяльності, її оцінці, аналітичній обробці первинних інформаційних матеріалів і поданні кінцевої інформаційної продукції відповідним інстанціям-споживачам.

ІАД складається з системи певних інформаційно-аналітичних робіт.

Інформаційно-аналітична робота (ІАР) – це комплекс заходів, які проводяться підрозділами служби безпеки підприємства з метою збору та обробки необхідних відомостей з ряду питань та на підставі проведеної роботи – розробки інформаційних (інформаційно-аналітичних) документів для керівництва підприємства.

Головні елементи ІАР:

– збір та пошук інформації (головний, самий важливий і визначаючий елемент);

– попереднє вивчення, інформаційно-аналітична обробка, формулювання висновків, облік;

– підготовка інформаційних (інформаційно-аналітичних) документів.

– інформаційна діяльність ґрунтується на застосуванні наукового методу. В основі методології інформаційно-аналітичного забезпечення безпеки підприємництва лежить методологія наукового пізнання.

1.2 Методологія інформаційного забезпечення фінансово-економічної безпеки діяльності підприємства.

Інформаційно-аналітичну діяльність можна умовно поділити на три рівні (стадії) – інформаційну, інформаційно-аналітичну (інформаційну аналітику) і науково-аналітичну. Вони розрізняються між собою не лише хронологічно, але і в структурно-функціональному плані. Причому за типами прикладної діяльності їх достатньо поділити на два види робіт: інформаційні технології першого рівня і власне інформаційно-аналітичну діяльність.

Інформаційні технології першого рівня – це наступні види діяльності: пошук, отримання, накопичення, трансляція первинної інформації. На цьому рівні відбувається пошук й виявлення інформації, первинне ознайомлення із здобутими матеріалами, попередній відбір цінних матеріалів і "відбракування" непотрібної інформації, формування баз даних і пошукових систем. Ця діяльність здійснюється безпосередньо у державних органах, а також в інформаційно-аналітичних підрозділах ОДВ. Саме на цьому рівні сьогодні широке поширення отримали автоматизовані системи на основі спеціальних науково-технічних і програмних продуктів і інформаційних технологій.

Власне ІАД спрямована на узагальнення, оцінку, зіставлення інформації, на її розуміння і інтерпретацію, на пояснення і розуміння інформації щодо об'єкту аналізу, прогнозування його поведінки, написання

рекомендацій для ухвалення управлінських рішень. Тому вона полягає в змістовній, системній, смисловій обробці інформації, конструюванні нового знання, діалектичному синтезі знань. На цьому рівні використовуються (при необхідності) так звані високі інтелектуальні інформаційні технології (ІІТ) з обробки інформації, моделювання (у тому числі комп'ютерне, імітаційне, аналогове). В ході цієї діяльності, як правило, здійснюється складання різних варіантів поведінки об'єктів, вироблення різних сценаріїв дій органів державної влади щодо управління ситуацією, вироблення рекомендацій і оцінок (у тому числі через пошук, отримання, накопичення, трансляцію, споживання первинної інформації), дослідження наслідків прийняття і реалізації управлінських рішень.

У процесі експертної та взагалі аналітичної діяльності також використовуються такі методи як: індивідуальна експертна оцінка, організація групових експертних процедур (нарада, метод «Дельфі», метод комісій (комітетів), ситуаційні кімнати і ін.), альтернативні сценарії, метод «суду», «мозкова атака», «ситуаційний аналіз», екстраполяція, ігри, когнітивні технології, генетичні алгоритми, еволюційні обчислення, історична аналогія, мережеві графи, аналіз мереж, дерево цілей (у тому числі метод «Патерн» як побудова дерева цілей і дерева рішень з вибором оптимальної стратегії), прогнозування, контекстуальне картографування, моделювання (аналогове, імітаційне, морфологічне, комп'ютерне, каузальне, статистичне, екстраполяційне), матричний метод (різновид аналогової моделі). Але вимогою якісного експертного аналізу є варіювання методів і експертних систем.

Існують спроби створення математичних моделей і комп'ютерних програм щодо підтримки аналітичної діяльності, проте, по-перше, вони недосконалі, по-друге, мають принципові обмеження у зв'язку з складністю раціоналізації аналітичних досліджень. Причому напрями аналітичних досліджень і очікування від них з боку органів держаної влади і осіб, що приймають рішення, поступово зміщуються у галузь консультацій, інтерпретації інформації, артикуляції зв'язності тенденцій і сценарного прогнозування, а саме переходять у площину конкретних технологій організаційного проектування стратегічного планування, інструментальної інженерії, іміджмейкингу, бренд-білдінгу, бенчмаркингу. У результаті усвідомлення обмеженості традиційних експертних досліджень для цілей перспективних і тактичних рішень в сучасних кризових соціальних умовах, саме ці технології стали новою стратегією «фабрик думки» на Заході.

Науково-аналітична діяльність у свою чергу полягає в системному аналізі конкретних об'єктів з метою пошуку і виділення загальних тенденцій їх розвитку, існуючих загроз, оцінки їх рівня, а також в прогнозуванні динаміки дії різних (у тому числі небезпечних) чинників на досліджуваний об'єкт, розробки сценаріїв можливого розвитку ситуації та вироблення механізмів і технологій щодо використання (у тому числі зменшенню небезпеки) різних чинників, доведенню цих механізмів і технологій до суб'єктів, здатних у тому числі надати позитивну дію на небезпечні чинники, або підсилити захисні механізми об'єкту.

До науково-аналітичної діяльності відноситься також розробка методології і методів ІАД, роботи з інформацією взагалі. Вирішення цих завдань передбачає проведення багатофакторного аналізу досліджуваної ситуації з врахуванням історії її розвитку, результатів досліджень схожих ситуацій, визначення і використання широкого спектру адекватних теоретичних підходів та евристичних прийомів. Ця діяльність здійснюється, як правило, спеціалізованими науковими підрозділами (НДІ, спеціалізованими аналітичними центрами тощо). Вся робота на цьому рівні будується на основі найбільш складних ІІТ і потребує високої кваліфікації. Міра досконалості ІІТ визначає глибину вирішення завдань та є інтелектуальним продуктом високого рівня, предметом конкуренції з іншими країнами.

Існують різні жанри і рівні аналітики. Жанри розрізняються за типами професійної аналітичної роботи (постановка аналітичного завдання, відбір та узагальнення інформації, аналіз поточної інформації, аналіз динаміки, підготовка підсумкових аналітичних документів тощо). Кожен жанр і рівень аналізу потребує як загальних для всіх умінь і навиків, так і специфічних для кожного з них. Загальними параметрами є: світогляд, цінності і цілі підприємства, в якому працюють аналітики, структура мислення, загальні навики і уміння працювати з інформацією. Іншими словами, необхідний системний підхід до організації інформаційно-аналітичної діяльності, її плановий і систематичний характер.

В зв'язку з цим очевидною є безліч науково-дослідних, науково-освітніх, науково-практичних завдань, у тому числі виробітку критеріїв і параметрів аналітичних продуктів (наукові критерії), параметрів експертизи аналітичних продуктів, джерел аналітичної інформації, вирішення проблеми зниження суб'єктивності експертів-аналітиків і підвищення рівня об'єктивності інформації, уточнення місця інформаційної аналітики в системі інформаційно-допоміжних видів діяльності. Необхідне соціальне позиціонування аналітики як проблеми методології організації інформаційно-аналітичного простору, його уніфікації тощо. В цьому зв’язку виникає дуже важлива проблема - доступність аналітичних продуктів для критики, а значить, вимога діяти на основі єдиних правил, тобто у рамках деякої уніфікованої сітки понять.

Аспекти інформаційно-аналітичних досліджень характеризується поділом інформації на загальнодоступну і службову:

1) «інформація для всіх», яка у свою чергу поділяється на: а) відволікаючу; б) направлену інформацію (орієнтовану на формування певної моделі суспільної свідомості, у тому числі за допомогою пропаганди); автором наголошується, наприклад, що характер направленої інформації може виступати як певний інформаційний сигнал (наприклад, такі ознаки, як кількість, частота, обсяг й ступень політичної напруженості інформації можуть бути ознаками майбутнього переходу від слів до справ — від пропаганди до активних політичних або військових дій);

2) інформація для вузьких груп (з грифами ДСК, «особливій важливості» і ін.). Сама логіка державного управління диктує необхідність відсікання основної маси громадян від інформації, що знаходиться в основі

управлінських процесів. Тому вся найбільш чутлива інформація щодо внутрішньополітичних і економічних питань, інформація МЗС, Міністерства оборони, спецслужб і т.д. є засекреченою. Будь-які конкретні політичні плани, перш їх закріплять у документах, проходять тривалий період обговорення на рівні ідей, пропозицій. У розвинених демократичних країнах участі в цих обговореннях приймають спеціальні групи фахівців-професіоналів.

3) наявність в інформаційних просторах «закритих зон», де інформація не має грифа секретності, але її розголошування небажане, і тому вона старанно ховається; іноді відбувається санкціонований виплеск закритої інформації.

Створення раціонального потоку інформації про економічну безпеку підприємства повинне опиратися на такі принципи ІАД:

– уніфікованості, що припускає те, що аналітики повинні прагнути до того, щоб проектні рішення, які ними пропонуються, підходили до якомога ширшого кола завдань, які вирішуються;

– системності, що припускає встановлення порядку функціонування всієї системи аналітичної інформації в цілому і її динамічних тенденцій;

– принцип вирішення нових завдань, що дозволяє виявляти й вирішувати нові завдання, які ставляться перед підприємством у зв'язку з ускладненням зовнішнього середовища;

– принцип першого керівника, заснований на безпосередньому керівництві аналітичною роботою на підприємстві першим керівником у зв'язку з тим припущенням, що він буде постійно націлювати аналітичний відділ на рішення нових більш складних завдань і намагатися вивести підприємство на лідируючі положення в конкурентному середовищі;

– принцип розвитку – розроблений комплекс вирішення аналітичних завдань повинен створюватися з урахуванням можливості поповнення й постійної актуалізації без порушення його функціонування;

– принцип сумісності – при створенні системи повинні бути реалізовані інформаційні інтерфейси, завдяки яким вона може взаємодіяти з іншими системами відповідно до встановлених правил;

– принцип стандартизації, що припускає те, що при створенні аналітичних комплексів повинні бути раціонально застосовані типові уніфіковані й стандартизовані елементи, проектні рішення, пакети прикладних програм, зокрема такі, які дозволяють займатися побудовою економіко-математичних моделей;

– принцип ефективності полягає у досягненні раціонального співвідношення між витратами й цільовими ефектами, включаючи кінцеві результати автоматизації;

– принцип єдиної інформаційної бази, що припускає те, що вихідна інформація один раз вводилась в систему й могла бути використана багаторазово.

Оцінка зовнішнього середовища ІАД підприємств здійснюється за допомогою: методу «5х5», методу «перелік з чотирьох питань», матриці Дж. Х. Вільсона, СВОТ-аналізу та СТЕП-аналізу. Під зовнішнім середовищем або середовищем функціонування ми розуміємо простір, що відображає сукупність

зовнішніх факторів прямого і непрямого впливу, що не перебувають у межах прямого безпосереднього впливу бізнес-процесів підприємств.

Для проведення наукового дослідження потрібна як первинна, так і вторинна інформація.

Первинна інформація – це вихідні дані, які є результатом конкретних експериментальних досліджень, вивчення практичного досвіду.

Вторинна інформація – це результат аналітико-синтетичної переробки первинної інформації.

Етап збору і відбору інформації для проведення наукових досліджень є одним із ключових. Організація його передбачає: визначення кола питань, що будуть вивчатись; хронологічні межі пошуку необхідної літератури; уточнення можливості використання літератури зарубіжних авторів; уточнення джерел інформації (книги, статті, патентна література, стандарти тощо); визначення ступеню відбору літератури - всю з даного питання, чи тільки окремі матеріали; участь в роботі тематичних семінарів і конференцій; особисті контакти із спеціалістами з даної проблеми; вивчення архівних документів, науково-технічних звітів; пошук інформації в Інтернеті.

Вихідну інформацію можна знайти в загальній і спеціальних енциклопедіях, а також у списках літератури, які прикладені до тематичних і оглядових робіт, що мають відношення до теми. В цьому випадку пошук інформації ведеться в антихронологічному порядку від більш пізніших джерел до більш ранніх. Такий шлях пошуку швидше приводить до поставленої мети.

При пошуку інформації слід дотримуватись певних принципів її формування, а саме:

– актуальність інформації має реально відображати стан об'єкта дослідження в кожен момент часу;

– достовірність – це доказ того, що названий результат є істинним, правдивим;

– інформація має точно відтворювати об'єктивний стан і розвиток об'єкта;

– інформаційна єдність, тобто подання інформації у такій системі показників, при якій виключалась би ймовірність протиріч у висновках і неузгодженість первинних і одержаних даних;

– релевантність даних, тобто одержання інформації за запитом користувача, включаючи роботу з даними, які не належать до дослідження.

Дотримання цих принципів дозволило б виключити дублювання наукових досліджень. За підрахунками американських спеціалістів, від 10 до 20% науково-дослідних робіт можна було б не проводити, якщо би правильно була підібрана наукова інформація з проблеми, яка вивчається.

Пошук потрібної інформації з кожним роком ускладнюється. Тому всі працівники мають знати основні положення інформаційного пошуку.

Інформаційний пошук – це сукупність операцій, спрямованих на пошук документів, які потрібні для розробки теми проблеми.

Інформаційні видання охоплюють усі галузі народного господарства. їх випускають інститути, служби НТІ, центри інформації, бібліотеки.

До основних інститутів і організацій України, які здійснюють централізований збір і обробку інформації основних елементів опублікованих документів, є: Книжкова палата України, Український інститут науково-технічної та економічної інформації (УкрУНТЕУ), Національна бібліотека України ім. В. І. Вернадського та інші бібліотечно-інформаційні установи загальнодержавного та регіонального рівнів.

Для підтвердження достовірності висновків і результатів дослідження, перевірки робочої гіпотези важливе значення має первинна інформація.

Найбільш поширеними і змістовними методами нагромадження первинної інформації є: опитування, спостереження, експеримент, тестування, анкетування.

Ефективним методом збирання первинної інформації є **аналіз документів.** Документи з різним ступенем повноти відображають економічний стан проблеми, фактологічну сторону соціальної дійсності; в них містяться відомості про процеси та результати діяльності підприємства, окремих людей, колективів, великих груп населення і суспільства в цілому. Саме з аналізу документів має розпочинатися конкретне дослідження.

Аналіз документів первинної і вторинної інформації дозволяє отримати об'єктивно існуючий стан і розвиток науки в цілому і окремих наукових напрямів. Вивчення наукових інформаційних потоків дає можливість планувати, прогнозувати тенденції розвитку науково-інформаційної діяльності і її удосконалення.

Дослідження документальних інформаційних потоків здійснюється за допомогою використання банку даних.

Банк даних – певна сукупність програмних, організаційних, технічних засобів призначених для централізованого накопичення та багатоцільового використання інформації, яка систематизована і сконцентрована в певному місті (у пам'яті ЕОМ, бібліотеці, каталогах, картотеці). Його ядром є база даних.

База даних – іменована сукупність інформаційних одиниць у певній предметній сфері. Функціонування цієї бази забезпечується сукупністю мовних і програмних засобів, які мають назву системи управління базою даних.

База даних сприяє формуванню бази знань.

База знань – сукупність систематизованих основних відомостей, що належать до певної галузі знань і зберігаються в пам'яті ЕОМ. У ній виокремлюється дві відносно самостійні частини: знання про певну галузь у вигляді термінів і законів, стверджень; конкретні, факти що описують цю галузь.

База знань сприяє розвитку бази даних.

Оцінка виникнення небезпечних ситуацій – ключова ланка визначення загального рівня безпеки підприємства. Існуючі методи оцінки виникнення небезпечних ситуацій можна поділити на феноменологічні, детерміністичні, імовірнісні та методи нелінійної динаміки й синергетики.

Феноменологічний метод базується на визначенні можливості протікання небезпечних фінансово-економічних процесів, виходячи з результатів аналізу необхідних і достатніх умов, пов’язаних з реалізацією тих

або інших заходів на підприємстві. Цей метод простий у застосуванні і дає надійні результати, якщо робочі стани і процеси такі, що можна з достатнім запасом визначити реальний стан компонентів розглянутої системи, і ненадійний поблизу границь різкої зміни стану виробництва і системи.

Детерміністичний метод передбачає аналіз послідовності етапів розвитку небезпечних фінансово-економічних процесів, починаючи від вихідної події через послідовність передбачуваних стадій відмовлень, деформацій і руйнування компонентів до сталого кінцевого стану системи. Хід потенційного небезпечного процесу вивчається і прогнозується за допомогою математичного моделювання, побудови імітаційних моделей і проведення складних розрахунків. Детерміністичний підхід забезпечує наочність і психологічну прийнятність, тому що дає можливість виявити основні фактори, які визначають хід процесу. Характерною його ознакою є побудова «дерева відмов».

Недоліки методу полягають в тому, що існує потенційна можливість не зафіксувати важливі, але рідкісні, ланцюжки фінансово-економічних подій. Побудова достатньо адекватних математичних моделей є дуже складним завданням навіть при сучасному розвитку обчислювальної техніки.

Імовірнісний метод аналізу небезпечних фінансово-економічних процесів вимагає як оцінки імовірності виникнення цих ситуацій, так і розрахунку можливого збитку від них. Оцінюються імовірності того або іншого шляху розвитку процесів. Імовірнісний метод передбачає аналіз послідовності етапів розвитку небезпечних фінансово-економічних процесів, починаючи від вихідної події через послідовність стадій відмов устаткування, поломки, деформації і руйнування компонентів системи, можливі технологічні причини, обумовлені порушенням режимів роботи функціонально пов'язаних систем. Якщо імовірність виникнення небезпечних фінансово-економічних процесів є неприйнятною величиною, то приймаються заходи для її зниження.

Методи нелінійної динаміки й синергетики в моделюванні небезпечних фінансово-економічних процесів роблять перші кроки. Катастрофічні економічні процеси – найбільш складні з досліджуваних динамічних процесів. Глибоке проникнення в природу виникнення небезпечних фінансово-економічних ситуацій, що відбуваються в підприємствах різних галузей, стало можливим завдяки теорії біфуркацій, яка виникла після того, як А. Пуанкаре ввів в математичний аналіз потужні топологічні і групові методи. Метод січних гіперповерхонь Пуанкаре дав дослідникам досить універсальний інструмент для вивчення багатомірних нелінійних об’єктів та їх дивної, на перший погляд, хаотичної поведінки.

У разі дослідження складних систем безпеки важливо відповісти на головне питання: коли система втрачає стан рівноваги і переходить з одного якісного стану в інший.

1.3 Політика інформаційної безпеки.

Інформація, будучи продуктом діяльності, виступає як власність держави, підприємств, установ, організацій, громадян, і, як об'єкт власності, вимагає захищеності. Проте проблема захисту інформації не зводиться тільки до захисту прав її власників, але і містить в собі такий важливий аспект, як захист прав громадян на вільний доступ до відомостей, гарантований конституцією. Основи захисту інформації розробляються органами державної влади, виходячи з умов забезпечення інформаційної безпеки зокрема і національної безпеки України в цілому.

Необхідною умовою нормального існування і розвитку кожного суспільства є захищеність від зовнішніх і внутрішніх загроз, стійкість до спроб зовнішнього тиску, як здатність протистояти таким спробам і нейтралізовувати виникаючі загрози, так і забезпечувати такі внутрішні і зовнішні умови існування країни, які гарантують можливість стабільного і всебічного прогресу суспільства і його громадян. Для характеристики цього стану використовується поняття національної безпеки.

Під **національною безпекою** слід розуміти стан захищеності життєво важливих національних інтересів від внутрішніх і зовнішніх загроз.

Система національних інтересів України визначається сукупністю основних інтересів особи, суспільства, держави і охоплює всі сфери їх діяльності: політичну, економічну, військову, екологічну, інформаційну, науково-технічну, соціальну та інші. Тому в змісті поняття "Національна безпека" можна виділити різні структурні елементи (компоненти), до основних з яких відносяться політична, економічна, військова, екологічна і інформаційна безпека.

Суть **політичної безпеки** полягає в здатності науки створити політичну систему, що забезпечує баланс інтересів різних соціальних груп; самостійно вирішувати питання державного устрою; проводити незалежну внутрішню і зовнішню політику.

Під **економічною безпекою** розуміється стан нації, при якому вона може суверенно, без зовнішнього втручання визначати шляхи і форми свого економічного розвитку.

Військова безпека полягає в можливості забезпечення національної безпеки засобами озброєного насильства. Насамперед військова безпека характеризується здатністю нації стримувати агресію або протидіяти їй.

Екологічна безпека полягає в наявності безпечного місця існування, що забезпечує нормальну життєдіяльність людини. Баланс компонентів у системі «населення – навколишнє середовище – природні ресурси» є гарантом життєздатності людського суспільства.

Інформаційна безпека – стан захищеності інформаційних ресурсів від внутрішніх і зовнішніх загроз, здатних завдати збитку інтересам особи, суспільства, держави (національним інтересам).

Оскільки в умовах інформатизації країни, розвитку інформаційних технологій, інформаційні ресурси формуються у всіх сферах діяльності, і

насамперед в політичній, військовій, економічній, науково – технічній, інформаційну безпеку слід розглядати як комплексний **показник** національної безпеки. Цим визначається її важливе місце і одна **з провідних ролей** в системі національної безпеки країни в сучасних умовах. Недарма існує ряд прислів'їв і виразів, що характеризують місце інформації в конкурентній боротьбі і в тактиці військових дій: «Хто володіє інформацією – той володіє ситуацією», «перемагає той, хто більш інформований про супротивника» та інші.

Основними загрозами інформаційній безпеці є просочування інформації і порушення її цілісності.

Забезпечення інформаційної безпеки здійснюється в рамках забезпечення національної безпеки.

Національна безпека досягається проведенням єдиної державної політики в області забезпечення безпеки, системою заходів економічного, політичного і іншого характеру, адекватних загрозам життєво важливих інтересів особі, суспільства і держави.

Політика України в області національної безпеки будується на основі «Стратегії національної безпеки України», затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015.

Дана стратегія визначає актуальні загрози національній безпеці Україні:

– агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території;

– неефективність системи забезпечення національної безпеки і оборони України;

– корупція та неефективна система державного управління;

– економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення;

– загрози енергетичній безпеці;

– загрози інформаційній безпеці;

– загрози кібербезпеці і безпеці інформаційних ресурсів;

– загрози безпеці критичної інфраструктури;

– загрози екологічній безпеці.

Серед основних напрямків державної політики національної безпеки України є наступні:

– відновлення територіальної цілісності України;

– створення ефективного сектору безпеки і оборони;

– підвищення обороноздатності держави;

– реформування та розвиток розвідувальних, контррозвідувальних і правоохоронних органів;

– реформування системи державного управління, нова якість антикорупційної політики;

– інтеграція в Європейський Союз;

– особливе партнерство з НАТО;

– забезпечення національної безпеки у зовнішньополітичній сфері;

– забезпечення економічної безпеки;

– забезпечення енергетичної безпеки;
– забезпечення інформаційної безпеки;
– забезпечення кібербезпеки і безпеки інформаційних ресурсів;
– забезпечення безпеки критичної інфраструктури;
– забезпечення екологічної безпеки.

Законодавчу основу забезпечення національної безпеки представляють Конституція України, закони України, укази Президента України, ухвали і розпорядження Кабінету Міністрів України, інші нормативно-правові акти державних органів влади і управління, прийняті у межах їх компетенції в даній сфері; міжнародні договори і угоди, поміщені або визнані Україною.

Основні положення і правові основи забезпечення національної безпеки закріплює Закон України «Про основи національної безпеки України». Він також визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Об'єктами національної безпеки є:

– людина і громадянин – їхні конституційні права і свободи;
– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;
– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність

Суб'єкти забезпечення національної безпеки є:

– Президент України;
– Верховна Рада України;
– Кабінет Міністрів України;
– Рада національної безпеки і оборони України;
– міністерства та інші центральні органи виконавчої влади;
– Національний банк України;
– суди загальної юрисдикції;
– прокуратура України;
– Національне антикорупційне бюро України;
– місцеві державні адміністрації та органи місцевого самоврядування;
– Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України;
– органи і підрозділи цивільного захисту;
– громадяни України, об'єднання громадян.

Основними принципами забезпечення безпеки є:

– пріоритет прав і свобод людини і громадянина;
– верховенство права;
– пріоритет договірних (мирних) засобів у розв'язанні конфліктів;
– своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам;

– чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки;

– демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки;

– використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

З розвитком інформаційних технологій постає питання, яким чином захистити інформацію. Всі напрями політики захисту інформації і інформаційних ресурсів реалізовані в Законодавстві України.

Законодавство в області захисту інформації включає:

– Цивільний кодекс України (частина 1 та частина 2);

– Кримінальний кодекс України;

– Розпорядження КМУ «Про схвалення стратегії розвитку інформаційного суспільства в Україні»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про державну таємницю»;

– Закон України «Про авторське право та суміжні права»;

– Закон України «Про національну програму інформатизації»;

– Закон України «Про друковані засоби масової інформації (пресу) в Україні».

В цілому розвиток законодавчої бази в області інформаційної безпеки йде по чотирьох основних напрямах:

– захист відомостей, що складають державну таємницю;

– захист конфіденційної інформації;

– захист авторського права у сфері інформатизації;

– захист права на доступ до інформації.

Органи забезпечення інформаційної безпеки в сукупності із законодавством утворюють державну систему інформаційної безпеки і захисту інформації.

Державна система захисту інформації включає:

– органи законодавчих, виконавчих і судових властей;

– законодавство, що регулює відносини в області захисту інформації і інформаційних ресурсів;

– нормативну правову базу по захисту інформації;

– служби (органи) захисту інформації підприємств, організацій, установ.

Основним органом управління державної системи захисту інформації є Державна служба спеціального зв'язку та захисту інформації в Україні Відповідно до своїх функцій вона здійснює:

– формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - інформаційно-телекомунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

– участь у формуванні та реалізації державної політики у сфері електронного документообігу в частині захисту інформації державних органів та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису, крім питань правового регулювання його застосування, в державних органах та органах місцевого самоврядування;

– забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Основним нормативно-правовим документом на основі якого функціонує Державна служба спеціального зв'язку та захисту інформації в Україні – це Закон України «Про Державну службу спеціального зв'язку та захисту інформації в Україні». Цей Закон відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації України.

1.4 Критерії безпеки інформаційних технологій.

1.4.1 Європейські критерії безпеки.

Країни Європи розробили погоджені «Критерії безпеки інформаційних технологій» (Information Technology Security Evaluation Criteria, далі – «Європейські критерії»). «Європейські критерії» розглядають такі задачі засобів інформаційної безпеки:

– захист інформації від несанкціонованого доступу з метою забезпечення її конфіденційності (підтримка конфіденційності);

– забезпечення цілісності інформації за допомогою захисту від її несанкціонованої модифікації чи знищення (підтримка цілісності);

– забезпечення працездатності систем за допомогою протидії загрозам відмовлення в обслуговуванні (підтримка приступності).

Для того щоб задовольнити вимогам конфіденційності, цілісності і доступності, необхідно реалізувати відповідний набір функцій безпеки, таких як ідентифікація й автентифікація, керування доступом, відновлення після збоїв і т.д. Щоб засоби захисту можна було визнати ефективними, потрібен високий

ступінь впевненості в правильності їхнього вибору і надійності функціонування. Для рішення цієї проблеми в «Європейських критеріях» уперше вводиться поняття ***адекватності*** (assurance) засобів захисту.

Адекватність містить у собі два аспекти: ***ефективність***, що відбиває відповідність засобів безпеки розв'язуваним задачам, і ***коректність***, що характеризує процес їхньої розробки і функціонування. Ефективність визначається відповідністю між задачами, поставленими перед засобами безпеки, і реалізованим набором функцій захисту – їхньою функціональною повнотою і погодженістю, простотою використання, а також можливими наслідками використання зловмисниками слабких місць захисту. Під коректністю розуміється правильність і надійність реалізації функцій безпеки (у прийнятій термінології – гарантування обраної ПБ).

У «Європейських критеріях» засоби, що мають відношення до інформаційної безпеки, розглядаються на трьох рівнях деталізації. На першому рівні розглядаються цілі, які переслідує забезпечення безпеки, другий рівень містить специфікації функцій захисту, а третій – механізми, що їх реалізують.

Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня адекватності їхньої реалізації.

Функціональні критерії

Специфікації функцій захисту пропонується розглядати з точки зору таких вимог: ідентифікація й автентифікація; керування доступом; підзвітність; аудит; повторне використання об'єктів; цілісність інформації; надійність обслуговування; безпека обміну даними.

Більшість з названих вимог збігається з аналогічними вимогами «Жовтогарячої книги». Зупинимося лише на специфічних для «Європейських критеріїв» моментах.

Вимоги безпеки обміну даними регламентують роботу засобів, що забезпечують безпеку даних, переданих по каналах зв'язку, і включають такі розділи: автентифікація; керування доступом; конфіденційність даних; цілісність даних; неможливість відмовитися від зроблених дій.

Набір функцій безпеки може специфікуватись з використанням посилань на заздалегідь визначені класи-шаблони. У «Європейських критеріях» таких класів десять. П'ять з них **(F-C1, F-C2, F-B1, F-B2, F-B3)** відповідають класам безпеки «Жовтогарячої книги» з аналогічними позначеннями. Інші п'ять класів розглянемо докладніше, тому що саме їхні вимоги відбивають точку зору розробників стандарту на проблему безпеки.

Клас **F-IN** призначений для систем з високими вимогами в забезпеченні цілісності, що типово для систем керування базами даних. Його опис заснований на концепції "ролей", що відповідають видам діяльності користувачів, і наданні доступу до визначених об'єктів тільки за допомогою довірених процесів. Повинні розрізнятися наступні види доступу: читання, запис, додавання, видалення, створення, перейменування і виконання об'єктів (мається на увазі породження суб'єкта з відповідного об'єкта-джерела).

Клас **F-AV** характеризується підвищеними вимогами до забезпечення працездатності системи. Це суттєво, наприклад, для систем керування

технологічними процесами. У вимогах цього класу вказується, що система повинна відновлюватися після відмови окремого апаратного компонента таким чином, щоб усі критично важливі функції постійно залишалися доступними. У такому ж режимі повинна відбуватися і заміна компонентів системи. Незалежно від рівня завантаження, повинен гарантуватися визначений максимальний час реакції системи на зовнішні події.

Клас **F-DI** орієнтований на розподілені системи обробки інформації. Перед початком обміну і при одержанні даних сторони повинні мати можливість провести ідентифікацію учасників взаємодії і перевірити її дійсність. Повинні використовуватися засоби контролю і виправлення помилок. Зокрема, при пересиланні даних повинні виявлятися усі випадкові чи навмисні перекручування адресної і користувальницької інформації. Знання алгоритму виявлення перекручувань не повинне дозволяти зловмиснику робити нелегальну модифікацію переданих даних. Повинні виявлятися спроби повторної передачі раніше переданих повідомлень.

Клас **F-DC** приділяє особливу увагу вимогам до конфіденційності переданої інформації. Інформація повинна передаватися по каналам зв'язку тільки в зашифрованому вигляді. Ключі шифрування повинні бути захищені від несанкціонованого доступу.

Клас **F-DX** висуває підвищені вимоги і до цілісності і до конфіденційності інформації. Його можна розглядати як функціональне об'єднання класів **F-DI** і **F-DC** з додатковими можливостями шифрування і захисту від аналізу трафіка. Повинен бути обмеженим доступ до раніше переданої інформації.

Критерії адекватності

«Європейські критерії» приділяють адекватності засобів захисту значно більше уваги, чим функціональним вимогам. Адекватність складається з двох компонентів – ефективності і коректності роботи засобів захисту.

Критерії ефективності

1. Відповідність набору засобів захисту проголошеним цілям.
2. Взаємна погодженість різних засобів і механізмів захисту.
3. Здатність засобів захисту протистояти атакам.
4. Можливість практичного використання недоліків архітектури засобів захисту.
5. Простота використання засобів захисту.
6. Можливість практичного використання функціональних недоліків засобів захисту.

Критерії коректності

– Процес розробки: специфікація вимог безпеки;розробка архітектури;створення робочого проекту; реалізація.

– Середовище розробки: засобу керування конфігурацією; використовувані мови програмування і компілятори; безпека середовища розробки.

– Експлуатаційна документація: керівництво користувача; керівництво адміністратора.

– Середовище розробки: доставка й установка; запуск і експлуатація.

«Європейські критерії» визначають сім рівнів адекватності – від **E0** до **E6** (у порядку зростання). Рівень **E0** позначає мінімальну адекватність. При перевірці адекватності аналізується весь життєвий цикл системи – від початкової фази проектування до експлуатації і керування. Рівні адекватності від **E1** до **E6** вишикувані по наростанню вимог старанності контролю. Так, на рівні **E1** аналізується лише загальна архітектура системи, а адекватність засобів захисту підтверджується функціональним тестуванням. На рівні **E3** до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення. На рівні **E6** потрібен формальний опис функцій безпеки, загальної архітектури, а також політики безпеки.

Ступінь безпеки системи визначається самим слабким з критично важливих механізмів захисту. У «Європейських критеріях» визначені три рівні безпеки – базовий, середній і високий. Безпека вважається: базовою, якщо засоби захисту здатні протистояти окремим випадковим атакам (зловмисник – фізична особа); середньою, якщо засоби захисту здатні протистояти зловмисникам, що володіють обмеженими ресурсами і можливостями (корпоративний зловмисник); високою, якщо є впевненість, що засоби захисту можуть бути подолані тільки зловмисником з високою кваліфікацією, набір можливостей і ресурсів якого виходить за рамки можливого (зловмисник – державна спецслужба).

1.4.2 Федеральні критерії безпеки інформаційних технологій США

Federal Criteria for Information Technology Security (FCITS) – стандарт інформаційної безпеки, розроблений Національним інститутом стандартів і технологій США (NIST) і Агентством національної безпеки США (NSA) у 90-х роках для використання в Американському федеральному стандарті з оброблення інформації (Federal Information Processing Standard), який повинен був замінити «Жовтогарячу книгу».

«Федеральні критерії» охоплюють практично весь спектр проблем, зв'язаних із захистом та забезпеченням безпеки, так як включають усі аспекти конфіденційності, цілісності та працездатності. Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій (IT-продукти) і системи оброблення інформації. Ключовим поняттям концепції інформаційної безпеки «Федеральних критеріїв» є поняття профілю захисту.

Цілі розробки

1. Визначення універсального і відкритого для подальшого розвитку набору основних вимог безпеки, пропонованих до сучасних інформаційних технологій.
2. Удосконалення існуючих вимог і критеріїв безпеки.
3. Приведення у відповідність між собою прийнятих у різних країнах вимог і критеріїв безпеки інформаційних технологій.
4. Нормативне закріплення основних принципів інформаційної безпеки.

Етапи розробки продукту ІТ.

1. Розробка й аналіз профілю захисту. Вимоги, викладені в профілі захисту, визначають функціональні можливості продуктів ІТ по забезпеченню безпеки й умови експлуатації, при дотриманні яких гарантується відповідність пропонованим вимогам. Профіль захисту аналізується на повноту, несуперечність і технічну коректність.

2. Розробка і кваліфікаційний аналіз продуктів ІТ. Розроблені продукти ІТ піддаються незалежному аналізу, мета якого – визначення ступеня відповідності характеристик продукту вимогам профілю захисту.

3. Компонування і сертифікація системи обробки інформації в цілому. Отримана в результаті система повинна задовольняти заявленим у профілі захисту вимогам.

4. Структура профілю захисту. Опис. Класифікаційна інформація, необхідна для ідентифікації профілю в спеціальній картотеці**. Обґрунтування.** Опис середовища експлуатації, передбачуваних загроз безпеки і методів використання продукту ІТ.

5. Функціональні вимоги. Реалізація політики безпеки. Політика аудита. Ідентифікація й автентифікація. Реєстрація в системі. Забезпечення прямої взаємодії з комплексом засобів захисту (КЗЗ). Реєстрація й облік подій. Політика керування доступом. Дискреційне керування доступом. Мандатне керування доступом. Контроль прихованих каналів. Політика забезпечення працездатності. Контроль за розподілом ресурсів. Забезпечення стійкості до відмов. Керування безпекою. Моніторинг взаємодій. Логічний захист КЗЗ. Фізичний захист КЗЗ. Самоконтроль КЗЗ. Ініціалізація і відновлення КЗЗ. Обмеження привілеїв при роботі з КЗЗ. Простота використання КЗЗ.

6. Вимоги до технології розробки

1. Процес розробки: визначення множини функцій КЗЗ відповідно до функціональних вимог; реалізація КЗЗ; визначення складу функціональних компонентів КЗЗ; визначення інтерфейсу КЗЗ; декомпозиція КЗЗ на функціональні модулі; структуризація КЗЗ на домени безпеки; мінімізація функцій і структури КЗЗ; адекватність реалізації КЗЗ; тестування й аналіз КЗЗ; тестування функцій КЗЗ; аналіз можливостей порушення безпеки; аналіз прихованих каналів.

2. Середовище розробки: інструментальні засоби; засоби керування процесом розробки; процедура дистрибуції.

3. Документування: документування функцій КЗЗ; повна документація на продукт ІТ (інтерфейси, компоненти, модулі, структура КЗЗ, методика проектування, а також вихідні тексти і специфікація апаратних засобів); документування тестування й аналізу продукту ІТ; документування процесу тестування функцій; документування аналізу можливостей порушення безпеки; документування аналізу схованих каналів; документування середовища і процесу розробки.

4. Супровід: користувальницька документація; посібник з адміністрування системи безпеки; процедура відновлення версій і виправлення помилок; процедура інсталяції.

7. Вимоги до процесу кваліфікаційного аналізу. Аналіз: Архітектури; Реалізації. Контроль: середовища розробки; процесу супроводу продукту ІТ. Тестування: функцій КЗЗ виробником; незалежне тестування функцій КЗЗ.

1.4.3 Міжнародний стандарт безпеки інформаційних технологій.

Навдемо основні поолження Міжнародного стандарту безпеки інформаційних технологій – ISO 15408.

Основні відомості

1. Регламентують усі стадії розробки, кваліфікаційного аналізу й експлуатації продуктів інформаційних технологій;

1. Пропонують досить складну і бюрократичну концепцію процесу розробки і кваліфікаційного аналізу продуктів ІТ.

Базові поняття.

Задачі захисту. Потреба споживачів продукту ІТ в протистоянні заданій множині загроз безпеці чи в необхідності реалізації політики безпеки.

Профіль захисту. Спеціальний нормативний документ, що представляє собою сукупність задач захисту, функціональних вимог, вимог адекватності і їхнього обґрунтування. Служить керівництвом для розроблювача при створенні проекту захисту.

Проект захисту. Спеціальний нормативний документ, що представляє собою сукупність задач захисту, функціональних вимог, вимог адекватності, загальних специфікацій засобів захисту і їхніх обґрунтувань. У ході кваліфікаційного аналізу служить як опис продукту ІТ.

Процес розробки і кваліфікаційного аналізу (рис. 1.2).

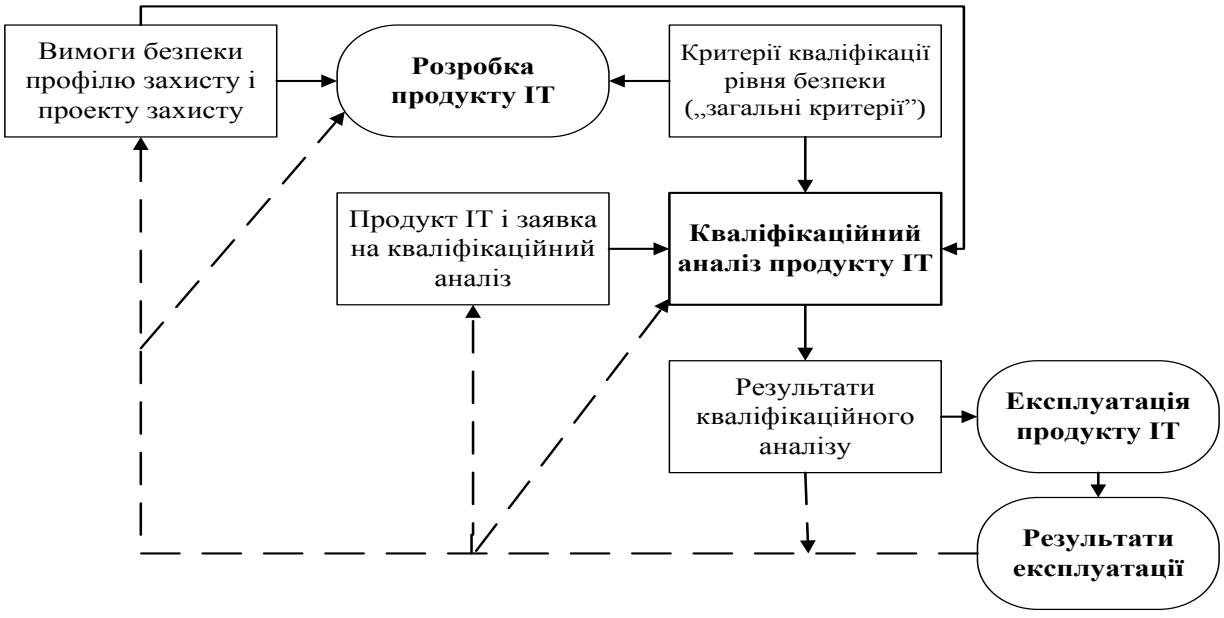

Рис. 1.2. Процес розробки і кваліфікаційного аналізу

Матеріали для проведення кваліфікаційного аналізу

1. Проект захисту, що описує функції захисту продукту ІТ і вимоги безпеки, що відповідають вимогам Профілю захисту, на реалізацію якого претендує продукт ІТ.
2. Докази можливостей продукту ІТ представлені його розроблювачем;
3. Продукт ІТ.
4. Додаткові відомості, отримані шляхом проведення різних експертиз.

Три стадії процесу кваліфікаційного аналізу

1. Аналіз профілю захисту на предмет його повноти, несуперечності, можливості реалізації і можливості використання як набір вимог для продукту, що аналізують.
2. Аналіз проекту захисту на предмет його відповідності вимогам профілю захисту, а також повноти, несуперечності, можливості реалізації і можливості використання як опису продукту ІТ.
3. Аналіз продукту ІТ на предмет відповідності проекту захисту.

Структура профілю захисту.

Введення. Інформація, необхідна для пошуку профілю в бібліотеці профілів. Ідентифікатор. Унікальне ім'я, придатне для пошуку серед подібних профілів і для посилань на нього.

Огляд змісту. Коротка анотація профілю захисту, на підставі якої споживач може зробити висновок про придатність даного профілю для його потреб.

Опис продукту ІТ. Коротка характеристика, функціональне призначення, принципи роботи, методи використання і т.д. Ця інформація не підлягає аналізу і сертифікації.

Середовище експлуатації. Опису всіх аспектів функціонування продукту ІТ, пов'язаних з безпекою. Загрози безпеці. Опис загроз безпеці, яким повинний протистояти захист. Для кожної загрози: джерело, метод впливу, об'єкт. Політика безпеки. Визначення і пояснення (при необхідності) правил політики безпеки. Умови експлуатації. Вичерпна характеристика середовища експлуатації з погляду безпеки.

Задачі захисту. Потреби користувачів у протидії зазначеним загрозам безпеці і/або в реалізації політики безпеки. Задачі захисту продукту ІТ. Інші задачі захисту.

Вимоги безпеки. Вимоги безпеки, яким повинний задовольняти продукт ІТ для рішення задач захисту.

Функціональні вимоги.

Тільки типові вимоги, передбачені відповідними розділами «Загальних критеріїв». Можуть наказувати чи забороняти використання конкретних методів і засобів.

Вимоги адекватності.

Також тільки типові вимоги.

Вимоги до середовища експлуатації.

Необов'язковий розділ. Функціональні вимоги і/або вимоги адекватності до середовища експлуатації. Використання типових вимог є бажаним, але не обов'язковим.

Додаткові відомості.

Необов'язковий розділ.

Обґрунтування.

Демонстрація того, що профіль захисту містить повну і зв'язну множину вимог, і що задовольняючий їм продукт ІТ буде ефективно протистояти загрозам безпеці середовища експлуатації.

Обґрунтування задач захисту

Демонстрація того, що задачі захисту, запропоновані в профілі, відповідають властивостям середовища експлуатації.

Обґрунтування вимог безпеки

Демонстрація того, що вимоги безпеки дозволяють вирішити задачі захисту, тому що:

– сукупність цілей, переслідуваних окремими функціональними вимогами, відповідає встановленим задачам захисту;

– вимоги безпеки є погодженими (не суперечать один одному);

– усі взаємозв'язки між вимогами враховані або за допомогою їхньої вказівки у вимогах, або за допомогою встановлення вимог до середовища експлуатації.

Структура проекту захисту.

Введення. Інформація, необхідна для ідентифікації проекту захисту, визначення призначення, а також огляд його змісту.

Ідентифікатор.

Унікальне ім'я, необхідне для пошуку й ідентифікації проекту захисту і відповідного йому продукту ІТ.

Огляд змісту.

Докладна анотація проекту захисту, на підставі якої споживач може зробити висновок про придатність продукту ІТ для рішення його задач.

Заявка на відповідність «Загальним критеріям»

Опис усіх властивостей продукту ІТ, що підлягають кваліфікаційному аналізу на основі «Загальних критеріїв».

Опис продукту ІТ. Середовище експлуатації: Загрози безпеці. Політика безпеки. Умови експлуатації.

Задачі захисту.

1. Задачі захисту продукту ІТ.
2. Інші задачі захисту.
3. Вищезазначені розділи збігаються з однойменними розділами профілю захисту.

Вимоги безпеки

Вимоги безпеки, якими керувався розроблювач продукту ІТ, що дозволяє йому заявляти про успішне рішення задач захисту.

Функціональні вимоги

На відміну від відповідного розділу профілю захисту, допускається використання крім типових вимог «Загальних критеріїв» інших, специфічних для даного продукту і середовища його експлуатації.

Вимоги адекватності

Може включати рівні адекватності, не передбачені в «Загальних критеріях».

Вимоги до середовища експлуатації

Необов'язковий розділ.

Загальні специфікації продукту ІТ.

Відображення реалізації продуктом ІТ вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту.

Специфікації функцій захисту

Опис функціональних можливостей засобів захисту продукту ІТ, що заявлені розроблювачем як ті, що реалізують вимоги безпеки. Форма представлення специфікацій повинна дозволяти визначати відповідності між функціями захисту і вимогами безпеки.

Специфікації рівня адекватності

Визначення заявленого рівня адекватності захисту продукту ІТ і його відповідність вимогам адекватності у вигляді подання параметрів технології проектування і створення продукту ІТ.

Заявка на відповідність профілю захисту.

Необов'язковий пункт. Проект захисту претендує на задоволення вимог одного чи декількох профілів захисту, для кожного з яких цей розділ повинний містити таку інформацію:

Посилання на профіль захисту

Однозначно ідентифікує профіль захисту, на реалізацію якого претендує проект захисту. Реалізація профілю захисту передбачає коректну реалізацію всіх його вимог без винятку.

Відповідність профілю захисту

Можливості продукту ІТ, що реалізують задачі захисту і вимоги, що містяться в профілі захисту.

Удосконалення профілю захисту

Можливості продукту ІТ, що виходять за рамки профілю.

Обґрунтування.

Демонстрація того, що проект захисту містить повну і зв'язну множину вимог, які покажуть, що реаліззуємий продукт ІТ буде ефективно протистояти загрозам безпеці середовища експлуатації і що загальні специфікації функцій захисту відповідають вимогам безпеки.

Обґрунтування задач захисту

Демонстрація того, що задачі захисту, запропоновані в проекті захисту, відповідають властивостям середовища експлуатації.

Обґрунтування вимог безпеки

Демонстрація того, що вимоги безпеки дозволяють вирішити задачі захисту, тому що:

1. Функціональні вимоги безпеки відповідають задачам захисту.
2. Вимоги адекватності відповідають функціональним вимогам і підсилюють їх.
3. Сукупність усіх функціональних вимог забезпечує рішення задач захисту.
4. Усі взаємозв'язки між вимогами «Загальних критеріїв» враховані або за допомогою зазначення їх у вимогах, або за допомогою встановлення вимог до середовища експлуатації.

Обґрунтування функцій захисту.

Демонстрація того, що функції захисту відповідають функціональним вимогам безпеки і задачам захисту. Повинно бути показано, що:

1. Зазначені функції захисту відповідають заявленим задачам захисту.
2. Сукупність зазначених функцій захисту забезпечує ефективне рішення сукупності задач захисту.
3. Заявлені можливості функцій захисту відповідають дійсності.

Обґрунтування рівня адекватності.

Підтвердження, що заявлений рівень безпеки відповідає вимогам адекватності.

Обґрунтування відповідності профілю захисту.

Демонстрація того, що вимоги проекту захисту підтримують усі вимоги профілю захисту. Повинно бути показане:

1. Всі удосконалення задач захисту в порівнянні з профілем захисту здійснені коректно й у напрямку їхнього розвитку і конкретизації.
2. Всі удосконалення вимог безпеки в порівнянні з профілем захисту здійснені коректно й у напрямку їхнього розвитку і конкретизації.
3. Усі задачі захисту профілю захисту успішно вирішені і усі вимоги профілю захисту задоволені.
4. Ніякі додатково введені в проект захисту спеціальні задачі захисту і вимоги безпеки не суперечать профілю захисту.

1.4.4 Українська нормативно-правова база щодо забезпечення фінансово-економічної безпеки.

Основними нормативно-правовими документами нашої країни в сфері фінансово-економічної безпеки є:

1. Закон України «Про доступ до публічної інформації».
2. Закон України «Про інформацію».
3. Закон України «Про захист інформації в автоматизованих системах».
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
5. Закон України «Про державну таємницю».

Сфера дії нормативних документів

Відповідно до закону України «Про інформацію», вся інформація поділяється на відкриту й інформацію з обмеженим доступом. Такий розподіл по режимах доступу здійснюється винятково на підставі ступеня конфіденційності інформації. Поряд з конфіденційністю важливими

характеристиками інформації є її цілісність і приступність, проте на сьогоднішній день іншої класифікації інформації, крім приведеної, не впроваджено.

Положення документів поширюються на державні органи, Збройні Сили, інші військові формування, МВС, а також підприємства, установи й організації усіх форм власності, що володіють, користаються і розпоряджаються інформацією, що є власністю держави, чи інформацією, захист якої гарантується державою.

Власники (користувачі) інформації, що не є власністю чи держави захист якої не гарантується державою, положення документів застосовують за своїм розсудом.

Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99)

Розглядаються 5 груп критеріїв:

1. Критерії конфіденційності.
2. Критерії цілісності.
3. Критерії доступності.
4. Критерії спостереженості.
5. Критерії гарантій.

Перші чотири групи складають функціональні критерії, які визначають, які послуги безпеки здатна надавати система, що оцінюється. До надання кожної з послуг безпеки висувається ряд вимог, за якими визначається рівень надання цієї послуги. Множина послуг безпеки, які надає система, складає так званий ***функціональний профіль захищеності.***

Критерії доступності

КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Критерії спостереженості

КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Критерії гарантій (Г-1…7):

1. архітектура
2. середовище розробки:

–процес розробки;

–керування конфігурацією.

3. послідовність розробки:

– функціональні специфікації (політика безпеки);
– функціональні специфікації (модель політики безпеки);
– проект архітектури;
– детальний проект.
4.реалізація
– середовище функціонування;
– документація;
– іспити комплексу засобів захисту.

Для реалізації деяких послуг безпеки необхідною умовою є реалізація інших послуг безпеки. Послуга безпеки НЦ (цілісність КЗЗ) є абсолютно необхідною. КС, в якій не реалізована послуга НЦ-1, не може вважатись захищеною, і профіль захищеності для такої системи взагалі не розглядається.

Контрольні питання:

1. Розкрити сутність понять: «інформаційний простір», « інформаційна війна», «інформаційна злочинність», «інформаційний вплив» та «інформаційна зброя».
2. Розкрийте сутність інформаційної безпеки.
3. Складові інформаційної безпеки.
4. Структура інформаційної безпеки.
5. Об’єкти інформаційної безпеки.
6. Сутність поняття «захисту інформації».
7. Економічна безпека підприємства: мета та завдання.
8. Складові інформаційно-аналітичне забезпечення безпеки підприємства.
9. Методологія інформаційно-аналітичного забезпечення безпеки підприємства.
10. Сутність інформаційно-аналітичної діяльності.
11. Сутність науково-аналітичної діяльність.
12. Загальнодержавна і службова інформація.
13. Принципи інформаційно-аналітичного діяльності.
14. Методи здійснення оцінки зовнішнього середовища при аналізі фінансово-економічної безпеки підприємства.
15. Сутність політики інформаційної безпеки.
16. Законодавча основа політики інформаційної безпеки.
17. Об’єкти та суб’єкти забезпечення національної безпеки.
18. Законодавство в області захисту інформації.
19. Критерії безпеки інформаційних технології.
20. Українська нормативно-правова база щодо забезпечення фінансово-економічної безпеки.

Тема 2. *Організація розробки системи аналітичного забезпечення фінансово-економічної безпеки на підприємстві*

План:

2.1 Визначення комплексної системи захисту інформації

2.2 Процес створення комплексної системи захисту інформації

2.3 Моделювання комплексної системи захисту інформації

2.4 Підготовка та оцінка ефективності комплексної системи захисту інформації

2.1 Визначення комплексної система захисту інформації.

Комплексні системи захисту інформації (КСЗІ) – сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації.

До складу комплексних систем захисту інформації включаються технічні засоби, призначені для побудови систем охоронної і пожежної сигналізації, систем управління протипожежною автоматикою, телевізійного спостереження, контролю і управління доступом, і що володіють технічною, інформаційною, експлуатаційною сумісністю і зв'язаних єдиною програмою, що управляє (системою збору і обробки інформації).

Будь-яка комплексна система захисту інформації є складною системою. Основні підсистеми КСЗІ:

– система контролю управління доступом;

– система відеоспостереження;

– система збору та обробки інформації;

– система протидії економічному шпигунству;

– система пожежної сигналізації;

– система автоматичного пожежогасіння.

Система охоронної сигналізації

Система охоронної сигналізації призначена для своєчасного сповіщення служби охорони, служби відділу позавідомчої охорони – у разі охорони об'єкту співробітниками позавідомчої охорони або здачі сигналізації на Пульт Централізованого Спостереження позавідомчої охорони – про проникнення (спробі проникнення), в будівлю або її окремі приміщення.

Як правило, дана система складається з:

– центрального комп'ютера;

– приймально-контрольних панелей;

– засобів виявлення;

– лінійної частини.

Система охоронної сигналізації повинна забезпечувати наступні функції:

– фіксацію факту і часу порушення рубежу охоронної сигналізації при його подоланні порушником (під подоланням рубежу охоронної сигналізації мається на увазі проникнення порушника на територію об'єкту, що охороняється, шляхом відкриття більш ніж на 100 мм або пролому дверей, відкриття або розбиття вікон при проникненні через віконні отвори, руйнування інших будівельних конструкцій, що підлягають устаткуванню засобами охоронної сигналізації, переміщення порушника в зоні дії приладів об'ємного виявлення) з одночасним відображенням інформації на пультах управління і на поетапних планах на моніторі персонального комп'ютера з вказівкою місця рубежу сигналізації, що спрацьовує;

– постановку і зняття зон з охорони: особистими паролями користувачів з пультів управління «встановлених» в своїх розділах; особистими паролями служби охорони з пультів, встановлених в приміщенні охорони; особистим паролем оператора системи охоронної сигналізації з автоматизованого робочого місця в приміщенні охорони.

– контроль стану шлейфів, датчиків, приладів з відображенням несправностей на моніторі комп'ютера;

– довготривале зберігання інформації для подальшого її відображення, роздрукування на принтері;

– відображення вхідних сигналів: «злом»; «пожежа»; «напад», «відновлення»; «тест»; «закриття»; «відкриття»; «несправність батареї»;

– відображення несправностей системи: відсутність мережі, несправність батареї, несправність телефонної лінії, несправність принтера;

– комп'ютер повинен працювати з сертифікованим програмним забезпеченням;

– контроль наявності на робочому місці оператора автоматизованого робочого місця з періодичним введенням особистого пароля.

Система контролю доступу.

Система контролю і управління доступом (СКУД) використовується для посилення охорони об'єкту і контролю допуску співробітників в службові і технічні приміщення об'єкту, а також управління евакуаційними дверима у разі аварійних ситуацій.

Вхід і вихід співробітників в дозволені зони доступності здійснюється по персоніфікованих електронних картах-пропусках в автоматичному режимі в дозволений час. Постійні (особисті) карти-пропуску виготовляються для співробітників і видаються їм в особисте користування. Код, записаний на карту-пропуск, є незмінним особистим кодом співробітника, з використанням якого він має можливість проходити в дозволені зони доступу і виділені приміщення, і на підставі якого ведеться автоматична реєстрація проходів.

При втраті карти-пропуску вводиться заборона на її використання.

Всі приміщення, залежно від призначення і характеру здійснюваних в них операцій, розділяються на зони по доступності.

Система контролю доступу об'єкту повинна забезпечувати:

– доступ в приміщення – по електронній карті-пропуску;

– доступ в приміщення – по електронній карті-пропуску і коду, що набирає на клавіатурі зчитувача;

– вихід з приміщень з використанням карти-пропуску або кнопки виходу;

– видачу сигналу тривоги в приміщення охорони (пультову) у разі несанкціонованого проникнення в зони доступу (злом, незакриття дверей; спроба підбору коду);

– примусове розблокування (з обов'язковим розбиванням захисного скла або автоматичне з пульта оператора) на випадок пожежі або іншій екстреній ситуації дверей евакуаційних виходів, якщо вони оснащуються засобами контролю доступу з реєстрацією цих фактів на сервері СКУД;

– облік, реєстрацію і документування фактів проходу співробітників в місцях установки пристроїв СКУД з вказівкою дати і часу проходу;

– створення і ведення бази даних на всіх співробітників, з введенням в неї паспортних і інших даних, кольорових фотографій, а також її оперативне коректування;

– доступ до бази даних і архіву, а також видачу довідок по ним з документуванням на принтері і екрані монітора оператора системи на вимогу користувача залежно від рівня доступу. Рівні доступу до бази даних і архіву системи визначаються замовником і можуть змінюватися в ході експлуатації системи;

– облік, реєстрацію і документування дій оператора;

– резервування журналу подій і бази даних співробітників на накопичувачі на магнітній стрічці.

До складу устаткування системи контролю доступу як правило входить наступне устаткування:

– робоче місце оператора СКУД (комп'ютер з монітором і принтером);

– дистанційні або інші зчитувачі;

– кнопки ручного розблокування дверей при виході з приміщень;

– локальні контролери управління і збору інформації;

– електромагнітні, електромеханічні замки;

– блоки живлення контролерів і замків;

– устаткування і програмне забезпечення для процесу виготовлення карт-пропусків і ведення бази даних;

– електронні ключі (картки).

Система відео спостереження.

Система відео спостереження призначена для візуального контролю обстановки по периметру об'єкту і в його внутрішніх приміщеннях засобами телевізійної техніки.

Система як правило включає:

– внутрішні і зовнішні (поворотні і стаціонарні) відеокамери для отримання відеозображення;

– пристрої обробки і перетворення відеозображення;

– апаратуру відеозапису і відтворення;

– апаратуру управління і комутації відеосигналів.

Система повинна забезпечувати запис візуальної і службової інформації від відеокамер на відеомагнітофони і проглядання цієї інформації як на телевізійних моніторах.

Система збору і обробки інформації.

Система збору і обробки інформації як правило виконується у вигляді інтегрованої системи, призначеної для управління системами безпеки будівлі і отримання інформації про стан всіх вхідних в неї підсистем. Система збору і обробки інформації повинна забезпечувати:

– інтеграцію всіх підсистем;

– зв'язок з підсистемами;

– автоматичне управління роботою підсистем;

– виконання команд оператора в безпечній для всіх технічних засобів і навколишніх осіб послідовності;

– прийом, реєстрацію і відповідну обробку тривожних сповіщень і сигналів, що поступають від підсистем;

– управління з робочих місць користувачів відповідно до функцій робочих місць;

– ієрархічний доступ операторів до функцій, ресурсів і інформації системи;

– внесення змін, модернізацію, заміну версій.

Система збору і обробки інформації складається з комп'ютерів автоматизованих робочих місць (АРМ) системи безпеки, серверів (основного і резервного) і, для підвищення надійності системи, окремої локальної обчислювальної мережі.

Програмне забезпечення системи збору і обробки інформації дозволяє здійснити виведення інформації про стан кожної вхідної в комплекс системи в графічному вигляді, з вказівкою поетапних планувань, місць розташування елементів системи і їх поточного стану в реальному масштабі часу.

Система протидії економічному шпигунству.

Система протидії економічному шпигунству повинна забезпечувати виявлення і локалізацію закладних пристроїв, вогнепальної холодної зброї, вибухових речовин, радіоактивних речовин і пристроїв, що містять речовини, які приховано проносяться на людині та її ручній поклажі.

До складу системи як правило входять пункти огляду і контролю на входах в будівлю (в'їздах на територію), які обладналися:

– стаціонарними металошукачами;

– стаціонарними пристроями детектування системи виявлення радіоактивних забруднень;

– ручними металошукачами;

– ручними дозиметрами;

– переносними рентгено-телевізійними інтроскопами;

– пристроєм локалізації вибухових речовин;

– комплектом для візуального огляду автомобілів.

Система повинна забезпечувати світлову і звукову сигналізацію виявлення небезпечних предметів.

Пункти огляду і контролю додатково обладнуються засобами зв'язку з черговою частиною і засобами охоронної сигналізації.

Концепція створення захищених комп'ютерних систем (КС).

При розробці і побудові комплексної системи захисту інформації в комп'ютерних системах необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, виробництва, експлуатації і розвитку таких систем. Системи захисту інформації відносяться до класу складних систем і для їх побудови можуть використовуватися основні принципи побудови складних систем з урахуванням специфіки вирішуваних завдань:

– паралельна розробка КС і система захисту інформації (СЗІ);
– системний підхід до побудови захищених КС;
– багаторівнева структура СЗІ;
– ієрархічна система управління СЗІ;
– блокова архітектура захищених КС;
– можливість розвитку СЗІ;
– дружній інтерфейс захищених КС з користувачами і обслуговуючим персоналом.

Перший з приведених принципів побудови СЗІ вимагає проведення одночасної **паралельної розробки КС і механізмів захисту.** Тільки в цьому випадку можливо ефективно забезпечити реалізацію решти всіх принципів. Причому в процесі розробки захищених КС повинен дотримуватися розумний компроміс між створенням вбудованих нероздільних механізмів захисту і блокових уніфікованих засобів і процедур захисту. Тільки на етапі розробки КС можна повністю врахувати взаємний вплив блоків і пристроїв власне КС і механізмів захисту, добитися системності захисту оптимальним чином.

Принцип системності є одним з основних концептуальних і методологічних принципів побудови захищених КС. Він припускає:

– аналіз всіх можливих загроз безпеці інформації;
– забезпечення захисту на всіх життєвих циклах КС;
– захист інформації у всіх ланках КС;
– комплексне використання механізмів захисту.

Комплексні системи захисту інформації завжди повинні мати **централізоване управління.** У розподілених КС управління захистом може здійснюватися за ієрархічним принципом. Централізація управління захистом інформації пояснюється необхідністю проведення єдиної політики в області безпеки інформаційних ресурсів в рамках підприємства, організації, корпорації, міністерства. Для здійснення централізованого управління в СЗІ мають бути передбачені спеціальні засоби дистанційного контролю, розподілу ключів, розмежування доступу, виготовлення атрибутів ідентифікації та інші.

Одним з важливих принципів побудови захищених КС є використання **блокової архітектури.** Застосування даного принципу дозволяє отримати цілий

ряд переваг: спрощується розробка, відладка, контроль і верифікація пристроїв (програм, алгоритмів); допускається паралельність розробки блоків; використовуються уніфіковані стандартні блоки; спрощується модернізація систем; зручність і простота експлуатації.

2.2 Процес створення комплексної системи захисту інформації (КСЗІ).

Система захисту інформації повинна створюватися спільно із створюваною комп'ютерною системою. При побудові системи захисту можуть використовуватися існуючі засоби захисту, або ж вони розробляються спеціально для конкретної КС. Залежно від особливостей комп'ютерної системи, умов її експлуатації і вимог до захисту інформації процес створення КСЗІ може не містити окремих етапів, або зміст їх може декілька відрізнятися від загальноприйнятих норм при розробці складних апаратно-програмних систем. Але зазвичай розробка таких систем включає наступні етапи: розробка технічного завдання; ескізне проектування; технічне проектування; робоче проектування; виробництво дослідного зразка.

Одним з основних етапів розробки КСЗІ є етап розробки технічного завдання. Саме на цьому етапі вирішуються практично всі специфічні завдання, характерні саме для розробки КСЗІ.

Процес розробки систем, що закінчується виробленням технічного завдання, називають науково-дослідною розробкою, а решту частини роботи із створення складної системи називають дослідно-конструкторською розробкою. Дослідно-конструкторська розробка апаратно-програмних засобів ведеться із застосуванням систем автоматизації проектування, алгоритми проектування добре вивчені і відпрацьовані. Тому особливий інтерес представляє розгляд процесу науково-дослідного проектування.

Науково-дослідна розробка КСЗІ.

Метою цього етапу є розробка технічного завдання та проектування КСЗІ. Технічне завдання містить основні технічні вимоги до КСЗІ, що розробляється, а також узгоджені взаємні зобов'язання замовника і виконавця розробки. Технічні вимоги визначають значення основних технічних характеристик, виконувані функції, режими роботи, взаємодія із зовнішніми системами і так далі

Апаратні засоби оцінюються наступними характеристиками: швидкодія, продуктивність, ємкість пристроїв, що запам'ятовують, розрядність, вартість, характеристики надійності і ін. Програмні засоби характеризуються необхідним об'ємом оперативної і зовнішньої пам'яті, системою програмування, в якій розроблені ці засоби, сумісністю з ОС і іншими програмними засобами, часом виконання, вартістю і так далі

Набуття значень цих характеристик, а також складу виконуваних функцій і режимів роботи засобів захисту, порядку їх використання і взаємодії із зовнішніми системами складають основний зміст етапу науково-дослідної

розробки. Для проведення досліджень на цьому етапі замовник може привертати виконавця або науково-дослідну установу, або організовує спільну їх роботу.

Науково-дослідна розробка починається з аналізу загроз безпеці інформації, аналізу КС, що захищається, і аналізу конфіденційності і важливості інформації в КС.

Перш за все проводиться аналіз конфіденційності і важливості інформації, яка повинна оброблятися, зберігатися і передаватися в КС. На основі аналізу робиться вивід про доцільність створення КСЗІ. Якщо інформація не є конфіденційною і легко може бути відновлена, то створювати КСЗІ немає необхідності. Не має сенсу також створювати КСЗІ в КС, якщо втрата цілісності і конфіденційності інформації пов'язана з незначними втратами.

У цих випадках досить використовувати штатні засоби КС і, можливо, страхування від втрати інформації.

При аналізі інформації визначаються потоки конфіденційної інформації, елементи КС, в яких вона обробляється і зберігається. На цьому етапі розглядаються також питання розмежування доступу до інформації окремих користувачів і цілих сегментів КС. На основі аналізу інформації визначаються вимоги до її захищеності. Вимоги задаються шляхом привласнення певного грифа конфіденційності, встановлення правил розмежування доступу.

Дуже важлива початкова інформація для побудови КСЗІ виходить в результаті аналізу КС, що захищається. Оскільки КСЗІ є підсистемою КС, та взаємодія системи захисту з КС можна визначити як внутрішнє, а взаємодія із зовнішнім середовищем – як зовнішнє.

Внутрішні умови взаємодії визначаються архітектурою КС. При побудові КСЗІ враховуються:

– географічне положення КС;
– тип КС (розподілена або зосереджена);
– структури КС (технічна, програмна, інформаційна і т. д.);
– продуктивність і надійність елементів КС;
– типи використовуваних апаратних і програмних засобів і режими їх роботи;
– загрози безпеці інформації, які породжуються усередині КС (відмови апаратних і програмних засобів, алгоритмічні помилки і тому подібне).

Враховуються наступні зовнішні умови:

– взаємодія із зовнішніми системами;
– випадкові і навмисні загрози.

Аналіз загроз безпеці є одним з обов'язкових умов побудови КСЗІ. За наслідками проведеного аналізу будується модель загроз безпеці інформації в КС. Модель загроз безпеці інформації в КС містить систематизовані дані про випадкові і навмисні загрози безпеці інформації в конкретній КС. Систематизація даних моделі припускає наявність відомостей про всі можливі загрози, їх небезпеку, тимчасові рамки дії, вірогідність реалізації. Часто модель

загроз розглядається як композиція моделі зловмисника і моделі випадкових загроз. Моделі представляються у вигляді таблиць, графів або на вербальному рівні. При побудові моделі зловмисника використовуються два підходи:

1) модель орієнтується тільки на висококваліфікованого зловмисника-професіонала, оснащеного всім необхідним і що має легальний доступ на всіх рубежах захисту;

2) модель враховує кваліфікацію зловмисника, його оснащеність (можливості) і офіційний статус в КС.

Перший підхід простіше реалізується і дозволяє визначити верхню межу навмисних загроз безпеці інформації.

Другий підхід відрізняється гнучкістю і дозволяє враховувати особливості КС повною мірою. Градація зловмисників по їх кваліфікації може бути різною. Наприклад, може бути виділено три класи **зловмисників:**

а) висококваліфікований зловмисник-професіонал;

б) кваліфікований зловмисник-непрофесіонал;

в) некваліфікований зловмисник-непрофесіонал.

Клас зловмисника, його оснащеність і статус на об'єкті КС визначають можливості зловмисника по несанкціонованому доступу до ресурсів КС.

Загрози, пов'язані з ненавмисними діями, добре вивчені, і велика частина їх може бути формалізована. Сюди слід віднести загрози безпеки, які пов'язані з кінцевою надійністю технічних систем. Загрози, що породжуються стихією або людиною, формалізувати складніше. Але з іншого боку, по ним накопичений великий об'єм статистичних даних. На підставі цих даних можна прогнозувати прояв загроз цього класу.

Модель зловмисника і модель випадкових загроз дозволяють отримати повний спектр загроз і їх характеристик. В сукупності з початковими даними, отриманими в результаті аналізу інформації, особливостей архітектури проектованої КС, моделі загроз безпеці інформації дозволяють отримати початкові дані для побудови моделі КСЗІ.

2.3 Моделювання комплексної системи захисту інформації.

Оцінка ефективності функціонування КСЗІ є складним науково-технічним завданням. Комплексна СЗІ оцінюється в процесі розробки КС, в період експлуатації і при створенні (модернізації) СЗІ для вже існуючих КС. При розробці складних систем поширеним методом проектування є синтез з подальшим аналізом. Система синтезується шляхом узгодженого об'єднання блоків, пристроїв, підсистем і аналізується (оцінюється) ефективність отриманого рішення. З безлічі синтезованих систем вибирається краща за наслідками аналізу, який здійснюється за допомогою моделювання.

Моделювання КСЗІ полягає в побудові образу (моделі) системи, з певною точністю відтворюючого процеси, що відбуваються в реальній системі. Реалізація моделі дозволяє отримувати і досліджувати характеристики реальної системи.

Для оцінки систем використовуються аналітичні і імітаційні моделі. У *аналітичних моделях* функціонування досліджуваної системи записується у вигляді математичних або логічних співвідношень. Для цих цілей використовується могутній математичний апарат: алгебра, функціональний аналіз, різницеві рівняння, теорія вірогідності, математична статистика, теорія множин, теорія масового обслуговування і так далі.

Для подолання цих складнощів застосовуються:

– спеціальні методи неформального моделювання;

– декомпозиція загального завдання на ряд окремих завдань;

– макромоделювання.

Спеціальні методи неформального моделювання.

Спеціальні методи неформального моделювання засновані на застосуванні неформальної теорії систем. Основними складовими частинами неформальної теорії систем є:

– структуризація архітектури і процесів функціонування складних систем;

– неформальні методи оцінювання;

– неформальні методи пошуку оптимальних рішень.

Структуризація є розвитком формального опису систем, поширеного на організаційно-технічні системи.

Прикладом структурованого процесу є конвеєрне виробництво. У основі такого виробництва лежать два принципи:

– строга регламентація технологічного процесу виробництва;

– спеціалізація виконавців і устаткування.

Вказані характеристики можуть бути отримані єдино доступними методами – методами ***неформального оцінювання.*** Суть методів полягає в залученні для отримання деяких характеристик фахівців-експертів у відповідних галузях знань.

Найбільшого поширення з неформальних методів оцінювання набули методи експертних оцінок. Методом експертних оцінок є алгоритм підбору фахівців-експертів, завдання правил отримання незалежних оцінок кожним експертом і подальшої статистичної обробки отриманих результатів. Методи експертних оцінок використовуються давно, добре відпрацьовані. В деяких випадках вони є єдино можливими методами оцінювання характеристик систем.

Неформальні методи пошуку оптимальних рішенні можуть бути розподілені по двох групах:

– методи неформального зведення складного завдання до формального опису і рішення задачі формальними методами;

– неформальний пошук оптимального рішення.

Макромоделювання.

При оцінці складних систем використовується також макромоделювання. Таке моделювання здійснюється для загальної оцінки системи. Завдання при цьому спрощується за рахунок використання при

побудові моделі тільки основних характеристик. До макромоделювання вдаються в основному для отримання попередніх оцінок систем.

На макрорівні можна, наприклад, досліджувати необхідне число рівнів захисту, їх ефективність по відношенню до передбачуваної моделі порушника з урахуванням особливостей КС і фінансових можливостей проектування і побудови КСЗІ.

Вибір показників ефективності і критеріїв оптимальності КСЗІ.

Ефективність систем оцінюється за допомогою показників ефективності. Іноді використовується термін – показник якості. Показниками якості, як правило, характеризують ступінь досконалості якого-небудь товару, пристрою, машини. Відносно складних людино машинних систем переважно використання терміну **показник ефективності функціонування,** який характеризує ступінь відповідності оцінюваної системи своєму призначенню.

Прикладом показника ефективності є криптостійкість шифру, яка виражається часом або вартістю злому шифру. Цей показник для шифру DES, наприклад, залежить від однієї характеристики – розрядності ключа. Для методів заміни кріптостійкість залежить від кількості використовуваних алфавітів заміни, а для методів перестановок – від розмірності таблиці і кількості використовуваних маршрутів Гамільтона.

2.4 Підготовка та оцінка ефективності комплексної системи захисту інформації.

Оцінка ефективності є важливим елементом розробки проектних і планових рішень, що дозволяє визначити рівень прогресивності діючої структури, розроблювальних проектів або планових заходів і проводиться з метою вибору найбільш раціонального варіанта структури або способу її вдосконалення. Ефективність захисних заходів (ЗМ) повинна оцінюватися на стадії проектування, для отримання найкращих показників працездатності системи в цілому.

У випадку ефективність ЗМ оцінюється як на етапі розробки, так і в процесі експлуатації системи захисту. В оцінці ефективності ЗМ, в залежності від використовуваних показників і способів їх отримання, можна виділити три підходи:

- класичний;
- офіційний;
- експериментальний.

Під класичним підходом до оцінки ефективності розуміється використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності виходять шляхом моделювання або визначаються за характеристиками реальної АС. Такий підхід використовується при розробці і модернізації КСЗІ. Проте можливості класичних методів комплексного оцінювання ефективності стосовно до ЗМ обмежені в силу ряду причин. Високий ступінь

невизначеності вихідних даних, складність формалізації процесів функціонування, відсутність загальновизнаних методик розрахунку показників ефективності та вибору критеріїв оптимальності створюють значні труднощі для застосування класичних методів оцінки ефективності.

Велику практичну значимість має підхід до визначення ефективності ЗМ, який умовно можна назвати офіційним. Політика безпеки інформаційних технологій проводиться державою і повинна спиратися на нормативні акти. У цих документах необхідно визначити вимоги до захищеності інформації різних категорій конфіденційності і важливості.

Під експериментальним підходом розуміється організація процесу визначення ефективності існуючих КСЗІ шляхом спроб подолання захисних механізмів системи спеціалістами, які виступають у ролі зловмисників. Такі дослідження проводяться таким чином. В якості умовного зловмисника вибирається один або декілька фахівців у галузі інформаційної боротьби найвищої кваліфікації. Складається план проведення експерименту. У ньому визначаються черговість і матеріально-технічне забезпечення проведення експериментів з визначення слабких ланок у системі захисту. При цьому можуть моделюватися дії зловмисників, які відповідають різним моделям поведінки порушників: від некваліфікованого зловмисника, що не має офіційного статусу в досліджуваній АС, до висококваліфікованого працівника служби безпеки.

Принципове значення для оцінок ефективності захисних заходів має вибір бази для порівняння або визначення рівня ефективності, який приймається за нормативний. Тут можна вказати кілька підходів, які можуть диференційовано використатися стосовно до конкретних випадків [23]. Один з них зводиться до порівняння з показниками, які характеризують ефективність організаційної структури еталонного варіанту системи захисту. Еталонний варіант може бути розроблений і спроектований з використанням всіх наявних методів і засобів проектування систем захисту, на основі передового досвіду і застосування прогресивних організаційних рішень. Характеристики такого варіанту приймаються як нормативних, при цьому порівняльна ефективність аналізованої чи проектованої системи визначається на основі зіставлення нормативних та фактичних (проектних) параметрів системи з використанням переважно кількісних методів порівняння. Може застосовуватися також порівняння з показниками ефективності та характеристиками системи управління, обраної як еталон, що визначає допустимий або достатній рівень ефективності організаційної структури.

Проте виникають деякі труднощі застосування зазначених підходів, які обумовлені необхідністю забезпечення порівнянності порівнюваних варіантів. Тому часто замість них використовується експертна оцінка організаційно-технічного рівня аналізованої і проектованої системи, а також окремих її підсистем і прийнятих проектних і планових рішень, або комплексна оцінка системи захисту, заснована на використанні кількісно-якісного підходу, що дозволяє оцінювати ефективність ЗМ по значній

сукупності факторів. Експертна оцінка може бути складовим елементом комплексної оцінки ефективності системи захисту, що включає всі перераховані підходи як до окремих підсистем, так і до системи в цілому.

Ефективність систем оцінюється за допомогою показників ефективності. Іноді використовується термін - показник якості. Показниками якості, як правило, характеризують ступінь досконалості будь-якого товару, пристрої, машини. Відносно складних людино-машинних систем переважніше використання терміна показник ефективності функціонування, який характеризує ступінь відповідності оцінюваної системи своєму призначенню.

Визначення показника ефективності можливо двома загальнонауковими методами:

- експериментом (випробуванням)
- математичним моделюванням (в даний час часто називають обчислювальним експериментом).

Стосовно до захисту інформації показники по значущості («знизу вгору») поділяються так: технічні - інформаційні (датчикової) - системні - надсістемние (ціннісні). Фізично, щодо захисту інформації від витоку, цей ряд виглядає так: сигнал / шум - ймовірність виявлення об'єкта - джерела інформації - імовірність його розкриття - збиток від витоку інформації. При цьому всі приватні показники між собою функціонально зв'язуються.

Для того щоб оцінити ефективність системи захисту інформації або порівняти системи за їх ефективності, необхідно задати деяке правило переваги. Таке правило або співвідношення, засноване на використанні показників ефективності, називають критерієм ефективності. Для отримання критерію ефективності при використанні деякого безлічі k-показників використовують ряд підходів. Зазвичай при синтезі системи виникає проблема виконання завдання з багатокритеріальним показником.

Ефективність КСЗІ оцінюється як на етапі розробки, так і в процесі експлуатації. У оцінці ефективності КСЗІ, залежно від використовуваних показників і способів їх отримання, можна виділити три підходи: класичний; офіційний; експериментальний.

У всіх розвинених країнах розроблені свої стандарти захищеності комп'ютерних систем критичного застосування. Так, в міністерстві оборони США використовується стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria), який відомий як Оранжева книга.

Згідно Оранжевій книзі для оцінки інформаційних систем розглядається чотири групи безпеки: A, B, З, D. В деяких випадках групи безпеки діляться додатково на класи безпеки.

Група А (гарантований або такий, що перевіряється захист) забезпечує гарантований рівень безпеки. Методи захисту, реалізовані в системі, можуть бути перевірені формальними методами. У цій групі є тільки один клас – А1.

Група В (повноважний або повний захист) представляє повний захист КС. У цій групі виділені класи безпеки В1,В2 і В3.

Клас B1 (захист через грифи або мітки) забезпечується використанням в КС грифів секретності, що визначають доступ користувачів до частин системи.

Клас B2 (структурований захист) досягається розділенням інформації на захищені і незахищені блоки і контролем доступу до них користувачів.

Клас B3 (області або домени безпеки) передбачає розділення КС на підсистеми з різним рівнем безпеки і контролем доступу до них користувачів.

Група З (виборчий захист) представляє вибірковий захист підсистем з контролем доступу до них користувачів. У цій групі виділені класи безпеки С1 і С2.

Клас С1 (виборчий захист інформації) передбачає розділення в КС користувачів і даних. Цей клас забезпечує найнижчий рівень захисту КС.

Клас С2 (захист через керований або контрольований доступ) забезпечується роздільним доступом користувачів до даних.

Групу D (мінімальній безпеці) складають КС, перевірені на безпеку, але які не можуть бути віднесені до класів А, В або З.

Організація захисту інформації в обчислювальних мережах міністерства оборони США здійснюється відповідно до вимог керівництва «The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines». Цей документ отримав назву Червона книга (як і попередній – за кольором обкладинки).

Подібні стандарти захищеності КС прийняті і в інших розвинених країнах. Так, в 1991 році Франція, Німеччина, Нідерланди і Великобританія прийняли узгоджені «Європейські критерії», в яких розглянуто 7 класів безпеки від Е0 до Е6.

Класи підрозділяються на чотири групи, що відрізняються якісним рівнем захисту: перша група містить тільки один сьомий клас; друга група характеризується дискреційним захистом і містить шостий і п'ятий класи; третя група характеризується мандатним захистом і з тримає четвертий, третій і другий класи; четверта група характеризується захистом і містить тільки перший клас.

Отже, **захист інформації** – це комплекс заходів, направлених на забезпечення інформаційної безпеки. Системи безпеки повинні не тільки і не стільки обмежувати допуск користувачів до інформаційних ресурсів, скільки визначати і делегувати їх повноваження в сумісному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації і усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів.

Контрольні питання:

1. Сутність комплексної системи захисту інформації.
2. Система охоронної сигналізації.
3. Система контролю доступу.
4. Система відео спостереження.
5. Система збору і обробки інформації.

6. Система протидії економічному шпигунству.

7. Концепція створення захищених комп’ютерних систем

8. Процес створення комплексних систем захисту інформації.

9. Науково-дослідна розробка комплексних систем захисту інформації.

10. Моделювання комплексних систем захисту інформації.

11. Методи моделювання комплексних систем захисту інформації.

12. Спеціальні методи моделювання комплексних систем захисту інформації.

13. Неформальні методи моделювання комплексних систем захисту інформації.

14. Вибір показників ефективності і критерії оптимальності комплексних систем захисту інформації.

15. Підготовка та оцінка ефективності комплексних систем захисту інформації.

Тема 3. *Фінансова безпека та фінансові інтереси підприємства*

План:
3.1 Сутність фінансової безпеки підприємства
3.2 Концепція фінансової безпеки підприємства
3.3 Алгоритм стрес-тестування підприємства
3.4 Механізм забезпечення фінансової безпеки підприємства

3.1 Сутність фінансової безпеки підприємства.

Для більш чіткого розуміння поняття фінансової безпеки підприємства та його ролі необхідно звернути увагу на те, що фінансова безпека є частиною системи економічної безпеки. В конкретному випадку можна навіть зробити висновок про те, що фінансова безпека підприємства є частиною фінансової безпеки регіону, яка, у свою чергу, входить у фінансову безпеку держави.

Наявність у складі економічної безпеки підприємства фінансової складової має суттєве методологічне і методичне значення. Поняття **«фінансова безпека підприємства»** має враховувати сутність фінансової безпеки держави, під якою розуміється такий стан фінансово-кредитної сфери держави, який характеризується збалансованістю і якістю системної сукупності фінансових інструментів, технологій і послуг, стійкістю до внутрішніх і зовнішніх негативних чинників (загроз), здатністю цієї сфери забезпечувати захист національних фінансових інтересів, достатні обсяги фінансових ресурсів для всіх суб'єктів господарювання і населення.

Фінансова безпека підприємства – це такий його фінансовий стан, який характеризується, по-перше, збалансованістю і якістю сукупності фінансових інструментів, технологій і послуг, що використовуються підприємством; по-друге, стійкістю до внутрішніх і зовнішніх загроз; по-третє, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів; по-четверте, забезпечувати ефективний і сталий розвиток цієї фінансової системи.

Умови забезпечення фінансової безпеки підприємства такі:

– високий ступінь гармонізації й узгодження фінансових інтересів підприємства з інтересами оточуючого середовища та інтересами його персоналу;

– наявність на підприємстві стійкої до загроз фінансової системи, яка спроможна забезпечувати реалізацію: фінансових інтересів, місії і завдань;

– збалансованість і комплексність фінансових інструментів і технологій, які використовуються на підприємстві;

– постійний і динамічний розвиток фінансової системи (підсистеми) підприємства.

Виходячи з усього вищесказаного, до понятійного апарату фінансової безпеки підприємства можна віднести такі основні категорії.

Об'єктом фінансової безпеки підприємства виступає фінансова діяльність підприємства, безпеку якої необхідно забезпечити (фінансова діяльність – це процес, на який спрямовується функціонування підсистеми забезпечення фінансової безпеки).

Суб'єкти фінансової безпеки – це керівництво підприємства і його персонал незалежно від займаних посад і виконуваних обов'язків.

Предмет фінансової безпеки підприємства полягає у діяльності суб'єктів фінансової безпеки як реалізації принципів, функцій, стратегічної програми або конкретних заходів з забезпечення фінансової безпеки, яка спрямована на об'єкти фінансової безпеки.

Основна мета забезпечення фінансової безпеки випливає із сутності фінансової безпеки підприємства і полягає у безперервному й сталому підтриманні такого стану фінансової діяльності, який характеризується збалансованістю і якістю всіх фінансових інструментів, технологій і фінансових послуг, які використовуються підприємством, стійкістю до впливу внутрішніх і зовнішніх загроз, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів, а також – розвиток цієї системи.

Ризик виступає однією з форм небезпеки, а саме:

а) можлива небезпека невдачі дій, що вживаються, або самі дії, пов'язані із такою небезпекою;

б) існування або можливість виникнення ситуації, за якої формуються передумови протидії реалізації цінностей, інтересів і цілей забезпечення безпеки;

в) можливість, яка спричиняє чи може спричинити невдачі запланованих дій та погіршити становище підприємства або спричинити його банкрутство (фінансовий ризик безумовно пов'язаний з управлінням підприємством і прийняттям для підприємства кардинальних рішень: будь-яке управлінське рішення – це вже ризик його реалізації і наслідків).

Поняття **«загроза»** є близьким за суттю і рівнем впливу на об'єкт загрози до терміну **«небезпека»**. Загроза виступає ще однією формою небезпеки, а саме: як небезпека на стадії можливого переходу у дійсність, як наявна чи потенційна демонстрація готовності:

а) щодо суб'єктів господарської діяльності – одних суб'єктів завдати шкоду іншим;

б) щодо процесів, явищ – негативно вплинути на господарську діяльність підприємства;

в) існування або можливість виникнення ситуації, за якої формується передумови протидії забезпеченню безпеки (вона обмежується діями, які підкріпляють її, але не переростають у діяльність, безпосередньо спрямовану на її здійснення);

г) сукупність причин та умов, які створюють небезпеку інтересам суб'єкта. Важливим методологічним положенням є визначення сутності і походження джерел небезпеки (загрози, ризику).

Джерела небезпеки – це потенційна можливість порушення функціонування та розвитку об'єкта. Такими джерелами є умови і чинники, вплив яких на об'єкт має негативний характер, або це умови й чинники, які містять у собі і за певних умов самі по собі або у різній сукупності виявляють чи знаходять ворожі наміри, шкідливі властивості, деструктивну природу.

В разі, коли рівень фінансової безпеки дуже низький або вона відсутня, на перший план виступає антикризове управління фінансовою діяльністю. Процес антикризового управління розпочинається тоді, коли на фінансову діяльність прямо діє сукупність певних загроз, але ще є можливість самостійно вийти з кризового стану. Під антикризовим управлінням розуміють систему управління підприємством, спрямовану на завчасне виявлення можливих кризових ситуацій, розроблення заходів протидії, швидке реагування на будь-які зміни в зовнішньому та внутрішньому середовищах.

Саме розробка і реалізація попереджувальних заходів у процесі антикризового управління є основою забезпечення фінансової стійкості підприємства. Основною метою обох видів управління (тобто антикризового і фінансовою безпекою) є повернення підприємства до нормального стану фінансової діяльності. Отже, об'єктом антикризового управління є кризовий фінансовий стан підприємства, об'єктом управління фінансовою безпекою — сукупність загроз і небезпек, які впливають на нього.

Різними є й інструменти, які використовуються цими видами управління:

– при антикризовому управлінні це: реструктуризація; реінжиніринг; санація;

– при управлінні фінансовою безпекою – методи стратегічного і поточного управління.

Індикатори або показники стану фінансової безпеки – це кількісні характеристики стану фінансової діяльності, відібрані для характеристики стану фінансової безпеки підприємства. Для останньої важливе значення мають як самі індикатори, що характеризують фінансовий стан, так і їхні порогові значення. Під пороговими значеннями індикаторів фінансової безпеки доцільно розуміти граничні величини, недотримання яких призводить до переходу фінансової безпеки з безпечного стану до небезпечного. Слід підкреслити, що за межами граничних значень індикаторів фінансової безпеки фінансова система підприємства втрачає спроможність до динамічного розвитку, стає об'єктом, який втрачає свою ліквідність, тому їй загрожує банкрутство.

Методом забезпечення фінансової безпеки підприємства виступає спосіб її забезпечення. Метод передбачає наявність інструменту фінансової діяльності, яким є певне фінансове знаряддя (фінансова технологія), що використовується в процесі реалізації відповідного методу.

Виходячи із загального розуміння терміна, принципом управління фінансовою безпекою підприємства слід вважати керівне положення, якого слід дотримуватися у процесі впливу на її стан.

До принципів управління фінансовою безпекою підприємства слід віднести такі:

– первинність господарського законодавства під час забезпечення фінансової безпеки підприємства;

– застосування програмно-цільового управління в забезпеченні фінансової безпеки підприємства;

– обов'язкове визначення сукупності власних фінансових інтересів підприємства у складі його місії;

– інтегрованість підсистеми управління фінансовою безпекою підприємства із загальною системою фінансового менеджменту;

– забезпечення збалансованості фінансових інтересів підприємства (в особі його власників і керівництва), окремих його підрозділів і персоналу, зайнятого на підприємстві;

– взаємна матеріальна відповідальність персоналу і керівництва за стан фінансової безпеки підприємства;

– необхідність постійного моніторингу реальних і потенційних загроз фінансовій безпеці;

– відповідність заходів із забезпечення фінансової безпеки економічній стратегії розвитку підприємства, його місії;

– координація між собою всіх вжитих заходів із забезпечення фінансової безпеки на підприємстві;

– необхідність і своєчасність удосконалення системи фінансової безпеки підприємства;

– необхідність організаційного і методичного оформлення підсистеми управління фінансовою безпекою;

– мінімізація витрат на забезпечення фінансової безпеки підприємства.

Важливим кроком на шляху забезпечення фінансової безпеки підприємства є розробка концепції фінансової безпеки.

3.2 Концепція фінансової безпеки підприємства.

Концепція фінансової безпеки – це певна сукупність поглядів на забезпечення фінансової безпеки, яка передбачає також комплексне визначення загроз і системне розуміння шляхів їх усунення. Концепція має включати шляхи виявлення й усунення загроз, принципи, які необхідно при цьому застосовувати, сукупність прогнозованих ситуацій зі станом фінансової безпеки, інструменти і технології, потрібні для цього, а також алгоритм забезпечення фінансової безпеки. Концепція як модель є основою для розробки стратегії забезпечення фінансової безпеки підприємства.

Прикладом такої концепції може бути «фінансова стратегія підприємства», яка визначається як «один із найбільш важливих видів функціональної стратегії підприємства, що забезпечує всі основні напрями розвитку його фінансової діяльності і фінансових відносин шляхом формування довгострокових фінансових цілей, вибору найбільш ефективних шляхів їхнього досягнення, адекватного корегування напрямів формування і використання фінансових ресурсів за зміни умов зовнішнього середовища».

Різновидом фінансової стратегії є стратегія забезпечення фінансової безпеки підприємства, яка може бути окремою системою, а може входити до складу загальної фінансової стратегії підприємства, яка, у свою чергу, входить до складу його загальної стратегії. Тоді стратегію забезпечення фінансової безпеки підприємства можна визначити так: це науково-методичний інструмент (технологія), який включає визначення стратегічних фінансових цілей (у вигляді фінансових інтересів), вибір ефективних напрямів, форм і методів їх досягнення й механізм реагування на зміни у зовнішньому середовищі і внутрішньому стані фінансової діяльності.

Основною метою такої стратегії має бути забезпечення фінансової безпеки підприємства.

Базуючись на підході до визначення сутності і змісту національних фінансових інтересів, до основних рис фінансових інтересів підприємства можна віднести такі:

– фінансові інтереси підприємства є проявом, з одного боку, економічних відносин підприємства, з іншого – суперечностей фінансової діяльності самого підприємства. У такому вигляді фінансові інтереси підприємства є носіями суперечностей фінансової діяльності і тому вони нерозривні між собою. Інтереси, як і суперечності, водночас є джерелами і рушіями розвитку фінансової діяльності підприємства і забезпечення його фінансової безпеки;

– фінансові інтереси підприємства породжені об'єктивною необхідністю повного забезпечення підприємства всіма видами фінансових ресурсів для здійснення ефективної комерційної (виробничої і маркетингової) діяльності. Фінансові інтереси на рівні підприємства – це відображення спільної думки власників, керівництва і персоналу підприємства, тобто є вираженням конкретних фінансових інтересів людей, які володіють або працюють на цьому підприємстві;

– структура фінансового інтересу підприємства містить об'єкт, тобто на що спрямований інтерес, і суб'єкт – хто конкретно має цей інтерес;

– фінансові інтереси проявляються у фінансовій діяльності підприємства і забезпечуються завдяки використанню певних фінансових інструментів (технологій);

– зміст фінансового інтересу підприємства поряд з основною метою його реалізації включає й засіб її досягнення, а саме, фінансовий інструмент як певну структуру, тобто між цими структурними елементами фінансового інтересу існує діалектична єдність.

Слід підкреслити, що за нинішніх умов розвитку економіки України одномоментна реалізація фінансових інтересів підприємства є неможливою. Така реалізація може бути тільки послідовною, а її тривалість обумовлюється наявністю жорстких ресурсних обмежень і конкуренцією на ринку. Це вимагає визначення пріоритетних завдань і рішучих дій керівництва й персоналу підприємства у ході їх виконання.

Існує головна (первинна) об'єктивна суперечність між стратегією розвитку підприємства, включаючи його операційну діяльність, і можливостями його

фінансового забезпечення. Дія цієї суперечності є рушієм фінансової безпеки підприємства.

Суб'єктами фінансових інтересів підприємства є: його власники, керівництво підприємства, персонал, тобто дотримується певна ієрархія фінансових інтересів підприємства. Загалом, фінансові інтереси є важливою складовою забезпечення розвитку підприємства й економічних відносин з оточуючим середовищем. Вони є об'єктивним виразом фінансової діяльності підприємства і провідною складовою економічних інтересів підприємства взагалі.

Реалізація фінансових інтересів тісно пов'язана із забезпеченням фінансової безпеки підприємства. По суті, реалізація фінансових інтересів підприємства і є змістом забезпечення його фінансової безпеки. Тому захист власних фінансових інтересів підприємства виступає найважливішою складовою забезпечення належного стану його фінансової безпеки.

Головний фінансовий інтерес підприємства у ринкових умовах – зростання його ринкової вартості та збільшення присутності на ринку.

До основних фінансових інтересів підприємства можна віднести:

1. максимізацію прибутку;
2. забезпеченість інвестиціями для розвитку підприємства, включаючи його фінансову систему і в її складі – підсистему забезпечення фінансової безпеки;
3. забезпечення основним і оборотним капіталом для ефективного ведення комерційної діяльності;
4. оптимізацію відрахувань до бюджету.

На рівень фінансової діяльності підприємства і, відповідно, на стан його фінансової безпеки впливають:

– внутрішні чинники – рівень операційного і стратегічного фінансового менеджменту;

– зовнішні чинники – держава, ринок, конкуренція.

Основні завдання підсистеми управління фінансовою безпекою підприємства такі:

– визначення пріоритетних фінансових інтересів підприємства і забезпечення їх коригування в разі необхідності;

– створення ефективного механізму забезпечення фінансової безпеки підприємства, умов оперативного реагування на загрози, їх своєчасного виявлення;

– прогнозування тенденцій, які ведуть до порушення нормального функціонування фінансової системи підприємства та її розвитку;

– встановлення причин і умов, які спричиняють фінансовий збиток і загрожують реалізації фінансових інтересів підприємства, порушенню нормального функціонування його фінансової системи;

– своєчасне виявлення й усунення загроз фінансовій безпеці підприємства, зниження ризиків у його фінансовій діяльності;

– забезпечення зацікавленості керівництва і персоналу в ефективній фінансовій діяльності підприємства;

– забезпечення відповідності визначених місії і фінансової стратегії підприємства сукупності його пріоритетних інтересів;

– забезпечення збалансованості фінансових інтересів окремих підрозділів і персоналу з пріоритетними фінансовими інтересами підприємства в цілому;

– створення умов для максимально можливого відшкодування або локалізації завданого збитку неправомірними діями юридичних чи фізичних осіб;

– проведення комплексу заходів із перевірки ділових партнерів даного підприємства;

– ефективне припинення зазіхань на фінансові ресурси з боку персоналу підприємства та його ділових партнерів.

При розробці і створенні підсистеми управління фінансовою безпекою підприємства доцільно дотримуватися таких вимог:

1. Підсистема управління фінансовою безпекою підприємства має функціонувати безперервно.

2. Підсистема повинна бути добре спланованою.

У межах певного підприємства має забезпечуватися не тільки функціональна самостійність цієї підсистеми, але й її інтегрованість до загальної системи управління підприємством.

3.3 Алгоритм стрес-тестування підприємства

Сучасний стан економіки України характеризується швидкими змінами умов функціонування підприємства, загрозами його фінансовим інтересам з боку окремих суб'єктів господарювання, високим рівнем фінансових ризиків. Тому важливим завданням щодо забезпечення життєздатності підприємства є гарантування його фінансово-економічної безпеки.

Серед методів, які дозволяють проводити ефективний аналіз рівня ризиків і стійкості підприємства до стресових явищ у економіці окремо можна виділити стрес-тестування. Використання стрес-тестування на підприємствах не фінансового сектору потребує розробки детальних методик і алгоритмів.

Головною перевагою проведення стрес-тестування є можливість кількісно оцінити негативний вплив критичних факторів ризику на фінансовий стан підприємства та розробити заходи протидії щодо мінімізації втрат. Стрес-тестування як метод оцінки ризиків у банківському секторі вперше запропоновано використовувати Міжнародним валютним фондом (МВФ), який разом з регуляторами і фінансовими інститутами різних країн проводив роботу з розвитку інструментів аналізу фінансової стабільності. Міжнародні органи, які регулюють банківську діяльність (Базельський комітет з банківського нагляду (Базель II), Банк Міжнародних Розрахунків, Центральний банк Росії [44]), і Національний банк України розробили рекомендації та методики щодо

проведення стрес-тестування в банківському секторі, з метою визначення підходів для здійснення «оцінки стабільності банківської системи або окремого банку за межами нормального операційного процесу та встановлення ступеня витривалості в разі виникнення екстремальних подій».

Практичне застосування стрес-тестування для оцінки ступеня схильності до ризику підприємств не набуло широкого розповсюдження. Хоча проведення стрес-тестування в умовах кризових процесів у економіці є досить доцільним, особливо на етапі затвердження нових інвестиційних проектів, чи стратегічних планів підприємства з метою мінімізації загроз стратегічної фінансової безпеки.

Стрес-тестування можна визначити, як оцінку потенційного впливу на фінансовий стан підприємства низки заданих змін у факторах ризику, які відповідають винятковим, але вірогідним подіям.

Метою стрес-тестування є оцінка стійкості підприємства до значних змін макроекономічного характеру й «екстремальним» подіям - малоймовірним, але все ж можливим кризовим ситуаціям, що важко піддаються прогнозуванню і в силу цього здатні призвести до аномально великих збитків (або прибутків).

Основним завданням за результатами стрес-тестування є підготовка упереджувальних стратегічних і тактичних заходів, які дозволять урегулювати проблемні або напружені ситуації, що можуть виникнути в майбутньому, та послабити вплив різних ризиків на діяльність підприємства.

Механізм проведення стрес-тестування включає такі основні елементи:

1. *Виявлення найбільш істотних ризиків, які можуть мати негативний вплив на фінансовий стан підприємства.*

Для ідентифікації ризиків здійснюються детальний аналіз структури балансу, доходів і витрат, ключових показників діяльності, в ході якого виявляються основні фактори ризику, що безпосередньо впливають на зміну фінансового стану підприємства.

Серед факторів ризику базовими можна визначити наступні:

1) макроекономічні категорії:

– стабільність економічної ситуації (економічний спад, радикальна зміна вектора розвитку економіки, дефолти компаній-позичальників; дефолти крупних поставщиків та покупців);

– значні коливання курсу національної валюти відносно інших валют (інфляція, дефляція);

– відкритість (доступність) банківського сектору, зміни відсоткових ставок та умов кредитування;

– рівень політичної та геополітичної стабільності;

– можливість знецінення майна, що перебуває як забезпечення за кредитними операціями банків (зокрема, через падіння цін на ринку нерухомості, кризу окремих галузей економіки тощо);

– волатильність цін на енергоресурси.

2) мікроекономічні категорії:

– конкурентна позиція підприємства.

Здійснюють аналіз динаміки факторів ризику, що склалася, шляхом визначення зміни їх значень на заданих відрізках часу.

2. Визначення методу проведення стрес-тестування.

При виборі методу проведення стрес-тестування в залежності від поставленої мети визначають тип стрес-тесту, який будуть використовувати (табл. 3.1). Поширенішими методами здійснення стрес-тестування є сценарний аналіз (далі - сценарій) і аналіз чутливості (далі - чутливість).

Сценарій стрес-тестування - це модель можливого розвитку подій під впливом різних факторів ризику. Сценарії стрес-тестування повинні охоплювати всі передумови, виникнення яких може завдати серйозних ударів по фінансовій стабільності підприємства.

Таблиця 3.1

Класифікація стрес-тестів

Найменування групи	*Види стрес-тестів*
За кількістю факторів ризику, що тестуються	однофакторні (аналіз чутливості)
	багатофакторні (сценарні)
За критерієм змін в часі	статичні
	динамічні
За методом побудови сценарію	гіпотетичні
	історичні
	змішані
За видами ризику, що тестується:	ризик зниження фінансової стійкості
	ризик неплатоспроможності
	ціновий ризик
	інфляційний ризик
	відсотковий ризик
	валютний ризик
	операційний ризик
	комплексний

Під час розроблення сценарію особливу увагу необхідно приділяти використанню факторів з максимально негативним впливом, що можуть призвести до подій, унаслідок яких підприємство може зазнати найбільших втрат та опрацювати варіанти найгіршого розвитку подій.

В роботі над ідентифікацією сценарію повинні брати участь експерти - керівники та співробітники підрозділів, які прогнозують фактори ризику. А сам процес розробки сценарію стрес-тестування рівня фінансової безпеки підприємства містить низку етапів, взаємозв'язок яких представлено на рис. 3.1.

Ефективність сценарного аналізу залежить від професіоналізму та підготовки експертів. Питання кадрового забезпечення передбачає відповідність освітньо-кваліфікаційних якостей працівників посаді, яку займаютє. Фахівець високого рівня сприяє економії часу при прийнятті рішень

і укладанні угод, реалізації нових проектів, зростанні прибутку та зниженню витрат підприємства, одночасно забезпечуючи фінансову безпеку суб'єкта підприємництва.

Експертні припущення та судження є неформалізованими, однак дуже вагомими складовими сценарію. У зв'язку з багатогранністю та складністю економічних процесів спеціалісти змушені оперувати загальними закономірностями та тенденціями з урахуванням історичних взаємозв'язків і спиратися на власні спостереження та досвід.

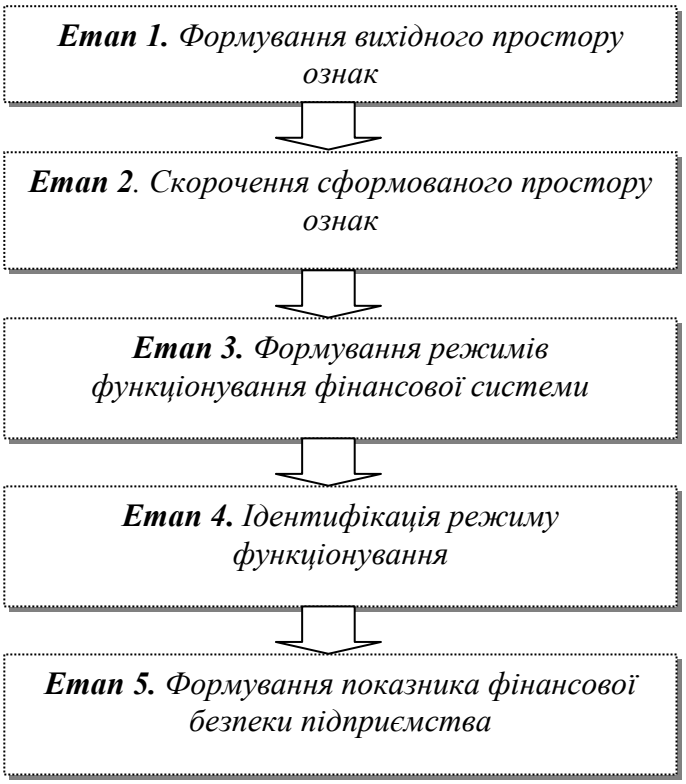

Рис. 3.1 Основні етапи розробки сценарію стрес-тестування рівня фінансової безпеки підприємства

Кожне підприємство залежно від галузі, діє в конкретному правовому полі, яке само по собі різноманітне. Внутрішнє поле складають організаційно-установчі документи, що визначають загальні напрямки розвитку, роботи підприємства, засади, організації облікової політики тощо. Зовнішнє коло законодавчого забезпечення складають нормативно-правові акти, положення та інструкції Верховної Ради, міністерств і відомств. Від можливості їх своєчасного інтерпретування, від їх сприяння підприємництву можлива реалізація першої перешкоди викривленням фінансової інформації та економічним зловживанням, що ставлять під сумнів конкретний фінансовий результат.

Стрес-тестування може базуватися на історичних сценаріях з використанням варіантів подій, що мали місце в минулому, або на гіпотетичних сценаріях, з використанням варіантів подій, які не відбувалися, але теоретично можуть статися.

Історичні сценарії не враховують усіх змін економічного середовища, які відбуваються з часом. За наявності певного ряду історичних даних можна розраховувати вірогідний діапазон можливих змін за допомогою методу математичної статистики.

Якщо історичних даних немає, то ймовірність змін доцільно визначати гіпотетично, відносно складових показника фінансової безпеки підприємства (табл. 3.2). Перевагами такого виду сценаріїв є можливості гнучкішого формулювання можливих криз, що дозволяє оптимізувати управління фінансовою безпекою суб'єкта господарювання.

Таблиця 3.2

Складові показника фінансової безпеки підприємства

Категорія, визначення, показники
Фінансова безпека - визначає граничний стан фінансової стабільності, в якому повинне перебувати підприємство для реалізації своєї стратегії. Характеризується здатністю підприємства протистояти зовнішнім і внутрішнім погрозам. Для оцінки фінансової безпеки запропоновані індикатори фінансової безпеки, головними з яких є показники зміни вартості підприємства
Фінансова гнучкість - здатність підприємства змінювати обсяг і структуру фінансування, а також напрямки вкладання фінансових ресурсів відповідно до внутрішніх обставин, що змінилися зовнішніми. Є якісною характеристикою, пропонується використовувати для її оцінки наявність управлінських опціонів у підприємства
Фінансова стабільність – визначається сталістю оптимальних або наближених до них значень показників. У якості показника фінансової стабільності пропонується використовувати значення середньоквадратичного відхилення (σ), розрахованого на основі відхилень фактичних значень показника від оптимальних. Тоді підприємство буде фінансово стабільним при виконанні наступної умови: $К_{опт.} = К_{факт.} \pm \sigma$, де: $К_{опт.}$, $К_{факт.}$ - оптимальні й фактичні значення фінансових коефіцієнтів, σ – середньоквадратичне відхилення
Фінансова рівновага – характеризує збалансованість розвитку підприємства, тобто досягається оптимальною комбінацією прибутковості й ризику.

З метою досягнення максимальної ефективності процесу, стрес-тестування доцільно здійснювати за кількома альтернативними сценаріями розвитку подій: позитивний, негативний, критичний.

Під час проведення стрес-тестування з використанням як історичних, так і гіпотетичних сценаріїв доцільне застосування різних ступенів впливу факторів ризиків: помірного, середнього, значного.

Сценарії стрес-тестування є ефективними, якщо вони: передбачають тільки суттєві зміни факторів; під час розрахунку результативних показників ураховують більшість базових факторів ризику; дозволяють отримати правдоподібні, на думку експертів, прогнозовані події із заданою ймовірністю їх виникнення.

Стрес-тестування чутливості полягає в дослідженні впливу на діяльність підприємства одного або кількох взаємопов'язаних факторів ризику. В разі використання цього підходу стрес-тестування здійснюють оцінку впливу миттєвої зміни одного фактора ризику, тоді як інші базові умови залишаються незмінними.

Доцільність застосування цього методу обумовлена можливістю оцінки значних зрушень без конкретних пояснень причин цих зрушень.

Показник чутливості визначає ступінь впливу окремого фактора ризику на діяльність підприємства залежно від змін, спричинених цим фактором. Чим вища чутливість, тим більше вплив цього фактора.

Хоча даному методу бракує історичного й економічного змісту, що в свою чергу може обмежувати його корисність для прийняття стратегічних рішень, тестування чутливості є важливим методом проведення оперативного стрес-тестування, результати якого важко переоцінити під час підготовки певних заходів щодо зменшення рівня ризику.

Прикладом стрес-тестування чутливості можуть служити негативні зміни відсоткових ставок за кредитами та/або депозитами на певну кількість базисних пунктів або падіння рівня цін на продукцію чи товар.

Визначення методики або алгоритму, які б дозволили спроектувати наслідки реалізації певного чинника ризику на діяльність підприємства.

Методики або алгоритми для кожного стрес-тесту складають окремо в залежності від мети й умов стрес-тестування.

1. Кількісний аналіз - розрахунок наслідків розвитку обраного сценарію за заданим алгоритму.

2. Інтерпретація отриманих результатів і прийняття управлінських рішень.

Результати стрес-тестування виносять на розгляд колегіальних органів управління підприємством з метою вибору методів та інструментів оптимізації (або мінімізації) ризиків і створення резервів під можливі втрати.

Аналіз результатів стрес-тестування є важливим не тільки з точки зору визначення рівня схильності до ризику підприємства, а і з практичної можливості спостереження й контролю рівня ризиків, які наражають підприємство на небезпеку, та ідентифікації найбільш серйозних загроз.

Під час здійснення аналізу необхідно враховувати, що стрес-тести не можуть охопити повний спектр і взаємодію ризиків, особливо це стосується операційного ризику і ризику, пов'язаного з порушенням законодавства.

Огляд результатів стрес-тестів можна здійснювати шляхом групування сукупного впливу стрес-тестів за видами ризиків та/або сценаріїв. Для підсумовування основних результатів (наприклад, відношення до капіталу або доходу) може бути використана структура очікуваних втрат.

Висновки щодо результатів стрес-тестування мають включати:

– короткий огляд ситуації щодо загального рівня фінансового стану підприємства;

– основні фактори ризику та припущення;

– результати стрес-тестування з зазначенням порушень установлених параметрів (показників і критеріїв);

– аналіз адекватності політики підприємства щодо управління та зменшення рівня ризику;

– рекомендації щодо прийняття управлінських рішень стосовно стратегічних чи оперативних планів підприємства.

Ключовим і завершальним етапом процесу стрес-тестування є розроблення заходів протидії в разі переходу негативних явищ і екстремальних подій з гіпотетичних до тих, що реально сталися. Розроблені заходи мають бути адекватнішими до рівня загрози й розміру потенційних збитків для підприємства. Особливо це стосується тих напрямів діяльності, де здійснення контролю за рівнем ризиків звичайними заходами ускладнюється. Ефективність розроблених заходів залежить від чіткого визначення умов, за яких вони повинні застосовуватися.

3.4 Механізм забезпечення фінансової безпеки підприємства.

Фінансова безпека досягається шляхом проведення виваженої фінансової політики відповідно до прийнятих у встановленому порядку доктрин, концепцій, стратегій і програм у політичній, соціальній, інформаційній і, власне, фінансовій сферах.

Розглянемо порівняльну характеристику підходів до механізму забезпечення фінансово-економічної безпеки під впливом екзогенних та ендогенних факторів, (табл. 3.3).

Таблиця 3.3

Порівняльна характеристика підходів до механізму забезпечення фінансово-економічної безпеки під впливом екзогенних та ендогенних факторів

Найменування підходу	*Мета*	*Засоби досягнення*	*Обмеження*
Фінансово-економічний	створення механізму забезпечення фінансової та економічної безпеки підприємств, і впливу на нього зовнішнього і внутрішнього середовищ	– виявляє і припиняє намагання конкурентів до здійснення недобросовісної конкуренції; – виявляє факти порушення договірних зобов'язань з боку партнерів-споживачів та постачальників продукції	відсутність всеосяжного та вчасного доступу до зовнішньої інформації
Контрозвітка, розвідка	забезпечення економічної безпеки підприємств з метою запобігання загрозам	протидія розвідувальним заходам, що носять превентивний характер (перевірка, контрозвідка, економічний (промисловий) шпіонаж, економічні війни	застосовується при наявності конкретного об'єкта небезпеки з чітко визначеною метою вчинення дій щодо настання несприятливих подій

Механізм забезпечення фінансової безпеки має реалізуватися на основі розробки відповідної наукової теорії, концепції, стратегії і тактики, проведення адекватної фінансової політики, визначення об'єктів, наявності необхідних інститутів забезпечення безпеки (суб'єктів), визначення та конкретизації інтересів, систематизації загроз, застосування засобів, способів і методів забезпечення безпеки (рис. 3.2).

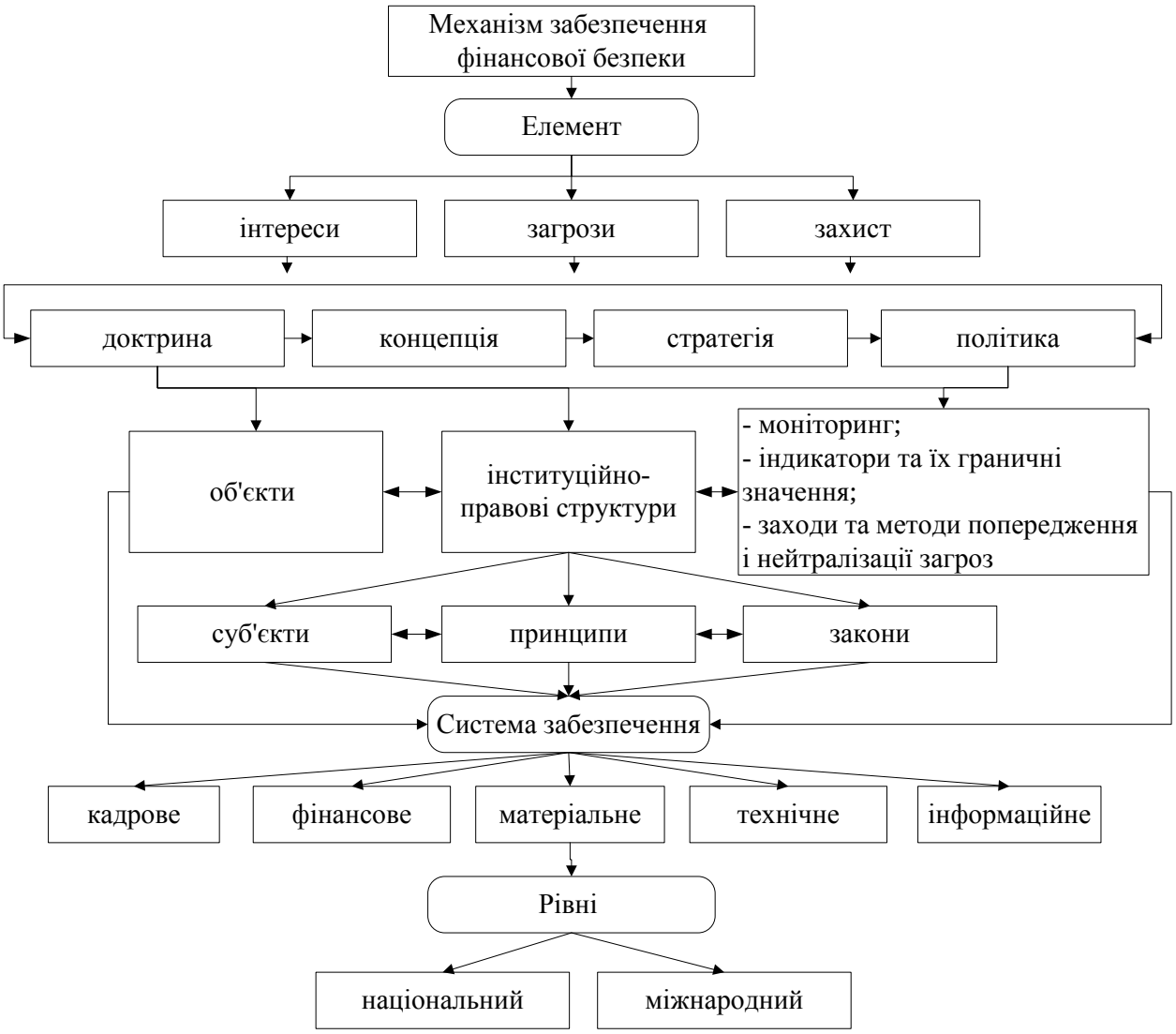

Рис. 3.2 Механізм забезпечення фінансової безпеки

Фінансова безпека забезпечується шляхом проведення виваженої фінансової політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, інформаційній і, власне, фінансовій сферах. Концепція фінансової безпеки має містити пріоритетні цілі і завдання забезпечення безпеки, шляхи та методи їх досягнення, які б адекватно відображали роль фінансів у соціально-економічному розвитку держави. Її зміст покликаний координувати загальнодержавні дії у сфері забезпечення безпеки на рівні окремих громадян, господарюючих суб'єктів, галузей, секторів економіки, а також на

регіональному, національному та міжнародному рівнях. Без обґрунтованої концепції фінансової безпеки неможливо сподіватись на реалізацію ефективного соціально-економічного розвитку держави.

Стратегія фінансової безпеки має бути орієнтована на розробку і послідовне здійснення заходів щодо закріплення і розвитку позитивних процесів і подолання негативних тенденцій у сфері фінансових відносин. При цьому мають бути визначені найближчі і перспективні цілі даної стратегії та механізми їх реалізації.

Державна стратегія фінансової безпеки і комплексна державна фінансова політика перебувають у тісному взаємозв'язку і взаємодії.

Зважаючи на те, що фінансова безпека не є статичною (на систему безпеки Впливає конкретна ситуація, що складається на певному етапі соціально- економічного і політичного розвитку суспільства), то механізм забезпечення фінансової безпеки включає такі елементи:

– об'єктивний і всесторонній моніторинг економіки і фінансової сфери з метою виявлення і прогнозування внутрішніх і зовнішніх загроз інтересам об'єктів фінансової безпеки;

– вироблення порогових, гранично допустимих значень фінансових та соціально-економічних показників /індикаторів/, перевищення яких може провокувати фінансову нестабільність і фінансову кризу;

– діяльність держави щодо виявлення і попередження внутрішніх і зовнішніх загроз фінансовій безпеці.

Таким чином, побудова механізму забезпечення фінансової безпеки потребує визначення критеріальних вимог до неї. Проте дотепер в економічній літературі відсутні теоретичні комплексні розробки цього питання. Тому за основу при формуванні критеріальних вимог до системи фінансової безпеки можна взяти підходи до визначення критеріїв та інтегрального індексу економічної безпеки за Методикою розрахунку рівня економічної безпеки України. Зазначена Методика розроблена з метою визначення рівня економічної безпеки України як головної складової національної безпеки держави і визначає перелік основних індикаторів стану економічної безпеки України, їхні оптимальні, порогові та граничні значення, а також методи розрахунку інтегрального індексу економічної безпеки. Методика базується на комплексному аналізі індикаторів економічної безпеки з виявленням потенційно можливих загроз економічній безпеці в Україні і застосовується Міністерством економіки України для інтегральної оцінки рівня економічної безпеки України в цілому по економіці та за окремими сферами діяльності. Відповідно дана Методика може використовуватись для моніторину окремих складових економічної безпеки з метою прийняття управлінських рішень щодо аналізу, попередження та нейтралізації реальних і потенційних загроз національним інтересам у відповідній сфері, і зокрема, фінансовій.

Механізм забезпечення фінансової безпеки має реалізовуватися на основі розробки відповідних наукової теорії, концепції, стратегії і тактики, проведення адекватної фінансової політики, визначення об'єктів, наявності

необхідних інститутів забезпечення безпеки (суб'єктів), визначення та конкретизації інтересів, систематизації загроз, застосування засобів, способів і методів забезпечення безпеки, (рис. 3.3).

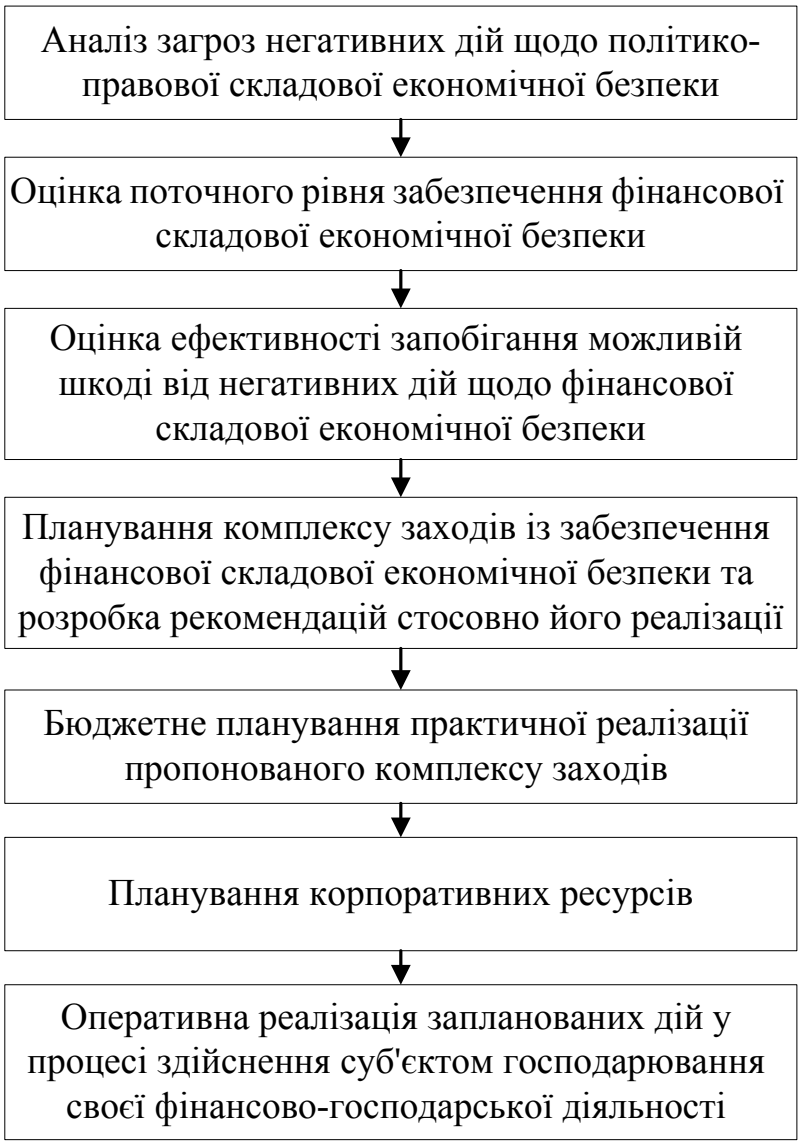

Рис. 3.3 Схема етапів забезпечення фінансової складової економічної безпеки підприємства

Концепція фінансової безпеки має містити пріоритетні цілі і завдання досягнення безпеки, шляхи та методи їх досягнення, які б адекватно відображали роль фінансів у соціально-економічному розвитку держави. Її зміст покликаний координувати загальнодержавні дії у сфері забезпечення безпеки на рівні окремих громадян, суб'єктів господарювання, галузей, секторів економіки, а також на регіональному, національному та міжнародному рівнях.

Механізм забезпечення фінансової безпеки підприємств з врахуванням можливостей використання зовнішнього середовища за умови впливу часового простору є важливим для суб'єкта господарювання, оскільки вимагає постійного моніторингу зовнішнього середовища та вчасної адаптації до своїх

внутрішніх інтересів, можливість запобігти зовнішнім загрозам, динаміки зміни поведінки та вчасне створення ряду запобіжних заходів з метою уникнення втрат прибутку або отримання збитку. Потрібно враховувати частоту та зміну динаміки, детермінованість факторів, факторний аналіз впливу на той чи інший суб'єкт, відносну швидкість та частоту. Необхідно відстежувати ке тільки зовнішні фактори в часовому просторі нанесені шкоди підприємству (партнерські зв'язки, конкуренти, посередники), а й вплив внутрішніх дій чи бездіяльності працівників самого господарюючого суб'єкта. Невчасна подача інформації чи перекрученість інформації, навмисне затримання може призвести до негативного піару, а, отже, як наслідок, до зниження рентабельності або банкрутства підприємства.

Контрольні питання:

1. Сутність фінансової безпеки підприємства.
2. Мета, предмет, об’єкти та суб’єкти фінансової безпеки підприємства.
3. Ризики фінансової безпеки підприємства.
4. Джерела небезпек для підприємства.
5. Принципи управління фінансової безпеки підприємства.
6. Сутність концепції фінансової безпеки підприємства.
7. Фінансові інтереси підприємства в контексті фінансової безпеки підприємства.
8. Суб’єкти фінансових інтересів підприємства.
9. Основа фінансових інтересів підприємства.
10. Завдання підсистеми управління фінансової безпеки підприємства.
11. Алгоритм стрес-тестування підприємства.
12. Мета та завдання струс-тестування підприємства.
13. Елементи струс-тестування.
14. Фактори ризику, які враховуються при стрес-тестування підприємства.
15. Класифікація стрес-тестів.
16. Основні етапи розробки сценарію стрес-тестування рівня фінансової безпеки підприємства.
17. Складові показника «фінансова безпека підприємства».
18. Механізм забезпечення фінансової безпеки підприємства.
19. Порівняльна характеристика підходів до механізму забезпечення фінансово-економічної безпеки під впливом екзогенних та ендогенних факторів.
20. Етапи забезпечення фінансової складової економічної безпеки підприємства.

Тема 4. *Фінансовий моніторинг та фінансова розвідка: закордонний та вітчизняний досвід*

План:
4.1 Система фінансового моніторингу
4.2 Форми організації системи фінансового моніторингу
4.3 Об'єктивна та суб'єктивна система фінансового моніторингу
4.4 Вітчизняна система фінансового моніторингу
4.5 Місце і роль фінансової розвідки у структурі економічної розвідки

4.1 Система фінансового моніторингу

Значною мірою успіх у діяльності з протидії легалізації «брудних» грошей визначається ефективністю системи фінансового моніторингу, запровадженої в країні. Моніторинг являє собою систему, ґрунтовану на постійному спостереженні за рівнем і станом кількісних та якісних показників з метою вивчення тенденцій.

Фінансовий моніторинг – це сукупність дій, спрямованих на протидію й запобігання легалізації грошей, отриманих злочинним шляхом, як в окремих суб'єктах господарювання, так і в масштабі всієї країни та за її межами.

Утім, поняття «протидія» щодо відмивання «брудних» грошей є ширшим за «запобігання». Важливість протидії зумовлена тим, що згідно із міжнародними та національними правовими актами відмивання грошей трактується як кримінальний злочин, ефективна боротьба з яким передбачає як кінцевий результат усунення злочину через покарання. В Україні відмивання грошей визнається кримінальним злочином згідно зі статтею 209 Кримінального кодексу України, ухваленого 5 квітня 2001 року № 2341–III, що набрав чинності 1 вересня 2001 року.

Під протидією відмиванню «брудних» грошей будемо розуміти комплекс таких завдань:

– встановлення кримінальної відповідальності за легалізацію (відмивання) «брудних» грошей;

– застосування адміністративних заходів, спрямованих на забезпечення ефективної системи боротьби з відмиванням грошей;

– заходи щодо покарання за вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів;

– вчинення процесуальних дій щодо справ про виявлення доходів, отриманих злочинними шляхом та з фінансування тероризму.

Під запобіганням слід розуміти запровадження радше превентивних заходів, які слід вживати з метою попередження й уникнення використання суб'єктів фінансового моніторингу, першою чергою фінансових посередників, для легалізації «брудних» коштів. З огляду на природу відмивання грошей механізми запобігання цьому явищу передусім мають бути запроваджені в тих суб'єктах, які функціонують у межах фінансового сектору.

Система заходів запобігання відмиванню грошей базується на таких основних принципах:

– встановлення мінімального рівня валютної1 операції, після якого всі операції такого роду підлягають реєстрації банківською (або іншою) установою з метою можливої подальшої перевірки;

– розроблення та введення в дію переліку ознак, які дають змогу визначити, чи належить здійснювана валютна операція до числа тих, що проводяться з метою відмивання грошей;

– встановлення відповідальності співробітників банківських (або інших фінансових) установ, через яких здійснюються фінансові операції, за інформування правоохоронних і контролюючих органів;

– проведення ідентифікації особи, яка здійснює фінансову операцію, що підлягає фінансовому моніторингу;

– забезпечення збереження документів, які стосуються ідентифікації осіб, котрі підлягають фінансовому моніторингу, та всієї документації про здійснення фінансової операції після проведення такої фінансової операції.

Систему фінансового моніторингу унаочнює рис. 4.1.

Рис. 4.1. Елементи фінансового моніторингу

Організація дієвої системи фінансового моніторингу передбачає вживання адміністративних заходів, серед яких, згідно з міжнародними конвенціями, вирізняють створення спеціальних уповноважених органів та підрозділів. У міжнародній практиці такі органи дістали назву «Підрозділи фінансової розвідки» (ПФР).

За визначенням Еґмонтської групи, фінансові розвідки – це центральні національні установи, відповідальні за отримання (а в окремих країнах – і за

вимогу) фінансової інформації, її аналіз і передання до компетентних органів, а також проведення слідства на її підставі.

Отже, повний комплекс повноважень органів, що становлять центр системи фінансового моніторингу, охоплює такі аспекти:

– отримання інформації від суб'єктів первинного фінансового моніторингу;

– оцінювання й аналіз отриманої інформації щодо фінансових операцій, які є об'єктом нагляду та контролю;

– проведення слідства щодо фактів, які свідчать про відмивання «брудних» грошей;

– передання узагальненої інформації до компетентних органів.

Таким чином, для вдосконалення управління фінансовою діяльністю необхідно організовувати систему моніторингу, розробити комплекс механізмів системи моніторингу фінансової діяльності підприємства, що дає змогу вчасно виявити відхилення фактичних результатів від прогнозованих, визначити причини відхилень і розробляти пропозиції щодо корегування окремих напрямків фінансової діяльності з метою її нормалізації та підвищення ефективності.

4.2 Форми організації системи фінансового моніторингу

За світовою практикою фінансові розвідки мають різні форми організації та повноваження. Форми організації фінансового моніторингу різняться підпорядкованістю головного уповноваженого органу та завданнями, які на нього покладені.

Вирізняють такі організаційні типи підрозділів фінансової розвідки:

– адміністративного типу, які діють самостійно або в складі міністерства фінансів чи центрального банку та не мають повноважень правоохоронних органів (наприклад, у Греції та Франції – при Міністерстві фінансів, а в Іспанії – при Банку Іспанії);

– «поліцейського» типу, які є складовою поліції (наприклад, Австрії – у структурі Міністерства внутрішніх справ, в Угорщині, Великій Британії, Швеції, Норвегії – у структурі Національної поліції);

– «прокурорського» типу, які є складовою органів прокуратури чи структурами міністерства юстиції (наприклад, у Данії – орган прокуратури, в Аргентині – при Міністерстві юстиції і прав людини, в Бельгії – Міністерство юстиції та фінансів);

– змішаного типу, які є поєднанням різних повноважень, унаслідок чого створюються під егідою різних організацій (наприклад, у Мексиці діє два органи: Генеральний директорат функціонує при Секретаріаті фінансів, а Агенція з боротьби з відмиванням грошей – при Офісі Генерального прокурора, в Німеччині запроваджено розподіл повноважень між різними органами, в Аргентині діє комісія, яка складається з представників різних відомств, причетних до протидії й запобігання відмиванню «брудних» грошей).

Переважають підрозділи фінансової розвідки поліцейського типу. Домінування цього типу зумовлене тим, що відмивання «брудних» грошей належить до кримінальних дій. Відповідно, кінцевого ефективного результату у протидії цьому злочину можна досягти шляхом порушення, розслідування кримінальних справ та його покаранням у правовому порядку. Ці оперативні заходи належать до інструментів поліції та правосуддя. Тим самим створюється повний цикл фінансового моніторингу: запобігання та протидія відмиванню (легалізації) незаконно отриманих доходів. Це є основною перевагою даного типу. Серед недоліків слід назвати певну закритість підрозділів фінансової розвідки для суспільства й надмірну концентрацію повноважень в «одних руках».

Другу позицію за поширеністю посідають системи адміністративного типу. Це зумовлене тим, що в боротьбі з легалізацією злочинних доходів вирішальна роль належить саме запобіганню злочину. Кінцевим об'єктом злочину є гроші, які функціонують, переміщуються з використанням фінансового сектору. Останній в системі адміністративного типу виступає ключовим елементом. Саме тому в країнах, які віддають перевагу запобіганню легалізації доходів, отриманих злочинним шляхом, підрозділ фінансової розвідки створюється у формі адміністративного органу – найчастіше як самостійна структура виконавчої влади, або при Міністерстві фінансів. Перевагою цього підходу є прозорість заходів системи фінансового моніторингу, встановлення контролю над цим явищем. Такий контроль має ґрунтуватися не лише і, мабуть, навіть не так на силових методах і прийомах, як спрямовуватися на створення науково обґрунтованої й придатної для практичного використання програми боротьби із відмиванням «брудних» грошей. Виходячи з цього, головним завданням підрозділів фінансової розвідки такого типу є аналітична та координаційна діяльність.

В організації оперативної й аналітичної роботи ПФР звернемо увагу на світовий досвід. У Великій Британії до аналізу банківської інформації, яка на рівних правах з інформацією, що надходить від агентури, розглядається як таємна (при цьому підозрювана особа ніколи не знає, що банк повідомив про свої підозри), допускаються лише офіцери, котрі мають спеціальну підготовку з банківсько-фінансової справи і законодавства, пов'язаного з цією сферою діяльності. У разі підозри організується тривале спостереження, а за необхідності – офіційне розслідування. За потреби ініціюють блокування й арешт коштів на відповідних рахунках. Із залученням відповідних експертів та використанням інформації з різних джерел працює Сектор оброблення фінансової інформації Бельгії. Крім того, за необхідності він має право призупиняти підозрілі фінансові операції для перевірки відомостей, але не більш як на 24 години. Водночас його співробітники самостійно не здійснюють слідчих дій. В Австрії у кожному банку працює спеціальний службовець , який має повідомляти про підозрілі операції. Така інформація приймається цілодобово черговою частиною відділу з боротьби з організованою злочинністю і відмиванням грошей. В Італії офіцери фінансової розвідки мають право

безперешкодного доступу на підприємства, у фірми, банки, до будь-яких документів для перевірки без дозволу на такі дії суду.

Існують інші класифікації систем фінансового моніторингу, а саме:

1) за характером впливу або повноваженнями можна виокремити:

– превентивні системи;

– регулювальні системи;

– каральні системи;

2) за рівнем управління

– одноріневі

– багаторівневі;

3) за характером мотивації інформування про підозрілі операції

– вимушені,

– примусові,

– ініціативні;

4) за критеріями звітування про фінансові операції

– об'єктивні (кількісні)

– суб'єктивні (якісні).

4.3 Об'єктивна та суб'єктивна системи фінансового моніторингу

Об'єктивна система звітування вперше з'явилась у США 1970 року з ухваленням Акту про звітування про валютні та іноземні трансакції. Зокрема, було запроваджено обов'язкове звітування фінансовими установами про всі валютні трансакції й трансакції грошових інструментів, які перевищують певну межу. Ця межа була встановлена на рівні $ 10000. Нині об'єктивну модель використовують в Австралії, Австрії, Бразилії, Коста-Ріці, Еквадорі, Норвегії, Парагваї та Венесуелі. Вона передбачає встановлення фіксованого порогу трансакції, за перевищення якого обов'язковим є звітування про всі внутрішні та міжнародні валютні операції.

Об'єктивна модель передбачає звітування про всі трансакції, які перевищують встановлену певну кількісну межу (рівень), з точки зору використання їх з метою відмивання грошей.

Основними перевагами такої системи є:

– створення відразливого ефекту для осіб, які мають намір відмити гроші, через ускладнення процесу відмивання;

– ефективний спосіб відстежування трансакцій;

– менші витрати на навчання персоналу фінансових установ щодо правильного дотримання вимог фінансового моніторингу.

За сучасних умов глобалізації та розвитку банківських технологій об'єктивна модель не в змозі ефективно, у повному обсязі запобігти відмиванню грошей, оскільки злочинці використовують здебільшого інформаційні технології для заплутування слідів, на відміну від депонування великих сум готівки, що було основним методом відмивання грошей у 1970х роках. Крім того, в межах об'єктивної моделі звіти, що справді акцентують увагу на

відмивання грошей, «губляться» у величезній кількості повідомлень про трансакції. Ще одне зауваження проти об'єктивної моделі міститься навіть у Сорока рекомендаціях ФАТФ стосовно збереження таємниці інформації, що надається фінансовими посередниками і надходить у розпорядження компетентних органів. Через звітування вразливими автоматично стають великі компанії1, що мають значний щоденний готівковий грошовий обіг, вищий за порогову межу. З огляду на це потрібні жорсткіші правила належного використання інформації. Через усі ці вади такої організації системи фінансового моніторингу вона не набула поширення у світовій практиці.

Розвиток міжнародної співпраці спричинив створення у 80-х роках минулого століття суб'єктивної моделі.

Суб'єктивна модель передбачає звітування про всі трансакції , які є підозрілими з точки зору використання їх з метою відмивання грошей .

Вимога, що встановлює механізм дослідження підозрілих трансакцій у межах суб'єктивної моделі, сформульована в Сорока рекомендаціях ФАТФ: «Фінансові установи мають звертати особливу увагу на будь-які складні, незвичайні великі операції та будь-які незвичайні схеми проведення операцій, які не мають очевидної законної кінцевої мети. Підґрунтя та цілі таких операцій мають бути досліджені якомога скоріше, встановлені дані слід зафіксувати письмово, щоб вони були доступними, аби допомогти наглядовим, аудиторським та правоохоронним органам». Як бачимо, ця модель не є чіткою, вона апелює такими характеристиками грошових трансакцій , як складні, незвичайно великі та незвичайні схеми проведення операцій. Вони не можуть розумітися всіма однозначно. Власне це і є найочевиднішою вадою даної системи. Попри це об'єктивна модель набула неабиякого поширення й запроваджена в Європі згідно із Директивою ЄС 91/3081.

Суб'єктивна модель складніша за об'єктивну; разом із цим вона вирізняється більшою ефективністю, оскільки активно залучає фінансові та не фінансові установи до запобігання відмиванню грошей, покладаючи на них велику відповідальність з виявлення «брудних» трансакцій та легалізації їх. Крім того, вона дає їм змогу ефективніше розподіляти свої ресурси, спрямовані на функціонування системи звітування, а також виходить із досвіду цих установ у розумінні діяльності своїх клієнтів та визначенні відповідності фінансової операції цій діяльності.

Серед вад цієї системи вирізнимо недостатність досвіду персоналу банку для визначення підозрілих трансакцій і нерівнозначне розуміння «підозрілості» трансакцій різними установами та фахівцями. Для послаблення цього недоліку ФАТФ рекомендує розробляти перелік критеріїв сумнівних операцій, щорічно його переглядати й доводити до відома фінансових установ.

Утім, у Німеччині законодавство не містить жодних ознак підозрілості трансакцій, про які необхідно повідомляти, зазначено лише, що це мають бути факти, які справді свідчать про відмивання грошей. Федеральний орган контролю за банками взагалі відмовився створювати такий каталог, наголосивши, що він може стати в нагоді особам, які здійснюють відмивання

грошей. Водночас у деяких країнах, наприклад у Швейцарії, ознаки підозрілих трансакцій закріплено в нормативно-правових актах.

Зараз винятково об'єктивну чи суб'єктивну модель не використовують у жодній країні. За світовим досвідом вимоги об'єктивної моделі застосовують, як правило, до готівкових операцій, а суб'єктивна модель використовується у сфері контролю передусім за безготівковими операціями, а також за підозрілими операціями із готівкою. В Канаді фінансові установи зобов'язані звітувати про операції з готівкою обсягом понад 100 тисяч канадських доларів, якщо вони здійснюються однією особою або для однієї особи впродовж одного дня. Крім того, банки повідомляють про всі підозрілі операції, пов'язані з відмиванням грошей. В Австрії, згідно із Директивами ЄС, обов'язковими є вимоги щодо ідентифікації учасника фінансової операції та пов'язаних із цим осіб, та вжиття заходів обачливості, якщо сума, на яку проводиться фінансова операція, дорівнює або перевищує 15000 євро або її еквівалент в іноземній валюті. До того ж, фінансові та не фінансові посередники зобов'язані надавати звіти про підозрілі операції до ПФР. І ще один приклад – Австралія, де не встановлено граничної межі, а передбачено зобов'язання банків і фінансових установ про інформування відповідного органу контролю країни про всі значні та підозрілі операції з готівкою. За безготівковими операціями банки мають самостійно сформувати критерії сумнівності.

4.4 Вітчизняна система фінансового моніторингу

Система фінансового моніторингу в Україні має дворівневу побудову (рис. 4.2). Згідно із Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» вона складається з первинного та державного рівнів. На першому рівні перебувають спеціально уповноважений орган виконавчої влади з питань фінансового моніторингу, центральні органи виконавчої влади і Центральний банк. Вони виконують функції регулювання та нагляду за діяльністю юридичних осіб, які забезпечують здійснення фінансових операцій.

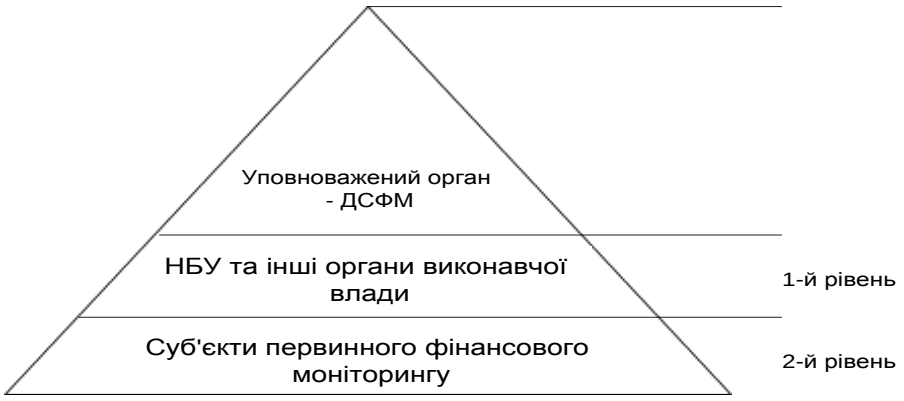

Рис. 4.2. Схема побудови вітчизняної системи фінансового моніторингу

Центральною ланкою вітчизняної системи фінансового моніторингу є Державна служба фінансового моніторингу, який виступає в ролі уповноваженого органу і координатора загальнонаціональної програми боротьби з легалізацією злочинних доходів і фінансуванням тероризму.

Діяльність Держфінмоніторингу спрямовується і координується Президентом та Кабінетом Міністрів України (рис. 4.3).

Рис. 4.3. Національна система України по боротьбі з відмиванням коштів

До базових нормативно-правових актів, що регламентують діяльність ДСФМ, першою чергою належить Закон України «Про запобігання та протидію

легалізації (відмиванню) доходів, отриманих злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

ДСФМ належить до підрозділів фінансової розвідки адміністративного типу. Він не має, так би мовити, «повного виробничого циклу» щодо виявлення фактів відмивання коштів, оскільки з-поміж основних етапів протидії відмиванню коштів (а саме первинне виявлення та реєстрація підозрілої інформації; аналіз інформації; розслідування справи) він здійснює аналіз отриманих повідомлень і в разі наявності підозр щодо відмивання коштів передає аналітичні довідки правоохоронним органам. Перший етап здійснюють суб'єкти первинного фінансового моніторингу. Розслідування справи в повному обсязі проводять правоохоронні органи на підставі інформації, отриманої від ДСФМ. Держфінмоніторинг відпрацьовує отримані повідомлення й у разі наявності підозр щодо відмивання коштів передає аналітичні довідки правоохоронним органам. Така система забезпечує прозорість процесу боротьби з відмиванням злочинних доходів, дає змогу надійно захищати банківську таємницю, зменшує ризик корупції та упереджених рішень. Разом із тим вона потребує кваліфікованих кадрів, суттєвих зусиль з боку координатора — ДСФМ та узгодження дій усіх учасників системи фінансового моніторингу.

Повноваження суб'єктів державного фінансового моніторингу.

Основними функціями ДСФМ є: отримання інформації від фінансових посередників, її аналіз, передання узагальнених матеріалів правоохоронним органам; координація дій інших учасників Національної системи протидії та запобігання легалізації (відмиванню) коштів, отриманих злочинним шляхом і фінансуванню тероризму; налагодження ефективної співпраці, взаємодії й інформаційного обміну з компетентними органами іноземних держав та міжнародними організаціями у зазначеній сфері.

Згідно із чинним законодавством, Держфінмоніторинг отримує інформацію від суб'єктів первинного фінансового моніторингу – професійних фінансових посередників. Комітет застосовує різні канали прийняття повідомлень: в електронному вигляді (від банківських установ за допомогою електронної пошти НБУ); на паперових носіях (від інших суб'єктів первинного фінансового моніторингу).

Крім спеціального уповноваженого органу фінансової розвідки до суб'єктів державного фінансового моніторингу, згідно зі статтею 5 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», належать Національний банк України, центральний орган виконавчої влади з формування та забезпечення реалізації державної політики у сфері запобігання і протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, Міністерство юстиції України, центральні органи виконавчої влади, що забезпечують формування державної політики у сфері надання послуг поштового зв'язку, у сфері економічного розвитку, Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне

регулювання у сфері ринків фінансових послуг, спеціально уповноважений орган. Вони надають інформацію ДСФМ на його вимогу в межах, визначених законодавством, та мають право отримувати від нього необхідну інформацію.

Суб'єкти первинного фінансового моніторингу та їхні повноваження.

Другий рівень системи фінансового моніторингу – це первинний моніторинг, який здійснюється фінансовими установами та іншими суб'єктами господарювання.

Відповідно до статті 5 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» до суб'єктів первинного фінансового моніторингу належать:

1) банки, страховики (перестраховики), страхові (перестрахові) брокери, кредитні спілки, ломбарди та інші фінансові установи;

2) платіжні організації, учасники чи члени платіжних систем;

3) товарні та інші біржі, що проводять фінансові операції з товарами;

4) професійні учасники фондового ринку (ринку цінних паперів);

5) оператори поштового зв'язку, інші установи, які проводять фінансові операції з переказу коштів;

6) філії або представництва іноземних суб'єктів господарської діяльності, які надають фінансові послуги на території України;

7) спеціально визначені суб'єкти первинного фінансового моніторингу:

а) суб'єкти підприємницької діяльності, які надають посередницькі послуги під час здійснення операцій з купівлі-продажу нерухомого майна;

б) суб'єкти господарювання, які здійснюють торгівлю за готівку дорогоцінними металами і дорогоцінним камінням та виробами з них;

в) суб'єкти господарювання, які проводять лотереї та азартні ігри, у тому числі казино, електронне (віртуальне) казино;

г) нотаріуси, адвокати, адвокатські бюро та об'єднання, аудитори, аудиторські фірми, суб'єкти господарювання, що надають послуги з бухгалтерського обліку, суб'єкти господарювання, що надають юридичні послуги (крім осіб, що надають послуги в рамках трудових правовідносин);

8) інші юридичні особи, які за своїм правовим статусом не є фінансовими установами, але надають окремі фінансові послуги.

Суб'єкти первинного фінансового моніторингу зобов'язані: проводити ідентифікацію особи, яка здійснює фінансову операцію, що підлягає фінансовому моніторингу, або відкриває рахунок (у тому числі депозитний), на підставі наданих в установленому порядку документів або за наявності підстав вважати, що інформація щодо ідентифікації особи потребує уточнення; забезпечувати виявлення і реєстрацію фінансових операцій, що підлягають фінансовому моніторингу; надавати Уповноваженому органу інформацію про фінансову операцію, що підлягає обов'язковому фінансовому моніторингу, не пізніше ніж упродовж трьох робочих днів від моменту реєстрації; сприяти працівникам Уповноваженого органу в проведенні аналізу фінансових операцій, що підлягають обов'язковому фінансовому моніторингу; надавати відповідно до

законодавства додаткову інформацію на запит Уповноваженого органу, пов’язану з фінансовими операціями, що стали об’єктом фінансового моніторингу, зокрема таку, що становить банківську та комерційну таємницю, не пізніше ніж упродовж трьох робочих днів від моменту отримання запиту; сприяти суб’єктам державного фінансового моніторингу з питань проведення аналізу фінансових операцій, що підлягають фінансовому моніторингу; вживати заходів щодо запобігання розголошенню (у тому числі особам, стосовно фінансових операцій яких проводиться перевірка) інформації, яка надається Уповноваженому органу, та іншої інформації з питань фінансового моніторингу (в тому числі про факт подання такої інформації); зберігати документи, які стосуються ідентифікації осіб, якими здійснено фінансову операцію, що підлягає фінансовому моніторингу, та всю документацію про здійснення фінансової операції упродовж п’яти років після проведення такої фінансової операції.

Крім того, суб’єкти первинного фінансового моніторингу мають встановлювати правила проведення внутрішнього фінансового моніторингу й призначати працівника, відповідального за його проведення.

4.5 Місце і роль фінансової розвідки у структурі економічної розвідки.

Під «фінансовою розвідкою» варто розуміти процес цілеспрямованого акумулювання та оброблення інформації з використанням системи методів та інструментів з метою забезпечення мінімізації загроз фінансовій безпеці суб'єктів господарювання. Економічна розвідка найбільш складна за своєю структурою за інші її види (політична, військової тощо), вона складається з промислової розвідки та комерційного шпигунства.

«Комерційне шпигунство» відокремлюється щодо: фінансових витрат, менеджменту, маркетингу. У його полі зору – розроблення конкурентом продукту, організації реклами, ринки збуту продукції тощо.

Промислова розвідка охоплює науково-технічне шпигунство, яке включає наукові дослідження, дослідно-конструкторських роботи, технології, організацію виробничих процесів; технологічне шпигунство, яке є найбільш результативним у короткостроковому періоді завдяки високим темпам науково-технічного прогресу; розвідку ресурсів, яка є потенційним джерелом високих доходів як в умовах високо-, так і низькотехнологічних виробництв.

Потрібно відрізняти поняття «фінансова розвідка» і «промислове шпигунство». «Промислове шпигунство» визначається як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність. Отже, «промислове шпигунство» відрізняється від «фінансової розвідки» тим, що воно збирає нелегальну інформацію, підкуп, шантаж, незаконне проникнення на територію конкурента, а фінансова розвідка збирає і користується тільки відкритою інформацією і загалом веде аналітичну діяльність, яка може впливати на розвиток бізнесу.

Фінансова розвідка опікується всією інформацією, що має життєво важливе значення і забезпечує переваги конкуренту, що стосується таких аспектів його господарської діяльності, як: розташовування ресурсів, процеси виробництва, технології, процеси розподілу і обігу, процеси споживання, процеси моделювання виробництва та економічних явищ.

Джерелами фінансової інформації можуть бути спеціалізована преса, звіти та внутрішні видання компаній, брошури і проекти, що перебувають у відкритому доступі. Близько 70-90 % всієї фінансової інформації можна отримати з відкритих джерел. Навіть оголошення про вакантної позиції дає змогу зробити низку висновків про діяльність компанії. Приміром, розміщена на інтернет-сайті підприємства вакансія фінансиста-аналітика для роботи, пов'язаної з постійними відрядженнями, може свідчити про те, що компанія планує вихід у регіони. А наявність вакансії регіонального представника вже не залишає в цьому ніяких сумнівів.

Серед найпоширеніших джерел інформації, якими користується фінансова розвідка, можна виділити такі:

а) публікації та звіти, отримані з відкритих джерел (Інтернет, преса, розсилаються прес-релізи). Незважаючи на те що інформація, отримана з цих джерел, не завжди містить усі необхідні дані, вона досить актуальна. Наприклад, відомості про виведення на ринок нової продукції можна знайти у спеціалізованій пресі задовго до її появи у продажу;

б) інформація, поширювана публічно, можна отримати проспекти, брошури, прайс-листи;

в) фінансова звітність, що публікується компаніями;

г) легальні бази даних державних установ, наявні у відкритому продажі.

д) аналіз виробів конкурентів, що перебувають у вільному продажу (оцінка фахівцями матеріалів, використаних у виробництві; технологій; аналіз функцій і вартості продукту).

Як правило, в довідку, підготовлену про конкурентів, входить така інформація:

– загальні відомості про компанію (адреса, керівництво, засновники, корпоративна історія);

– фінансова інформація (річний фінансовий звіт за останні три роки, обсяг виробництва, аналіз зовнішньоекономічної діяльності);

– характеристика діяльності компанії;

– окремі події, факти (дані про участь компанії в офіційних заходах, арбітражі, судових розглядах);

– рейтинг стану компанії, що відображає фінансове становище і ступінь ризику при співпраці з цією компанією;

Чинниками, які забезпечують ефективність функціонування економічної розвідки, є:

1. Реалізація розвідки (саме яким чином).
2. Розподіл ролей та відповідальності за реалізацію заходів.
3. Розповсюдження інформації на підприємстві.

4. Уявлення щодо економічної розвідки як до довгострокового проекту, який не надає миттєвих результатів.

5. Формулювання і концентрування на ключових питаннях.

Діяльність підрозділу економічної розвідки виконує подвійну функцію: забезпечує фінансову безпеку підприємства і вирішує маркетингові задачі, оскільки на засадах одержуваної інформації виробляється господарська політика фірми.

Служба розвідки на підприємстві створюється з метою:

– управління ризиками бізнесу;

– раннього виявлення загроз, можливостей, уразливих місць та інших негативних факторів впливу на успіх бізнесу;

– забезпечення конкурентних переваг продукції підприємства на ринку за рахунок своєчасного прийняття нестандартних оптимальних керівних рішень.

Фінансова розвідка створює нову "базу знань" для підприємства, яка охоплює: розвиток власної групи експертів, фінансову інформацію щодо конкурентів, результати аналітичних досліджень.

До питань, що можуть зацікавити розвідку у фінансовій сфері, належать: інформація про планові і фактичні показники фінансового плану; майнове становище; вартість товарних залишків (для конкурентів, під час визначення кредитоспроможності та надійності як партнера); стан банківських рахунків; банківські операції та зв'язки; грошові обороти; фінансові операції; планові та звітні показники за валютними операціями; рівень виручки і доходів; боргові зобов'язання (перевірка партнерів); стан балансу (активи та пасиви); розміри і умови банківських кредитів; інформація про розміри запланованого кредитування; генеральна стратегія й тактика у валютних і кредитних питаннях; інформація з питань кредитних і валютних відносин з іноземними державами та фірмами.

У штатному розкладі підрозділ фінансової розвідки може діяти у рамках служби безпеки компанії або під будь-якою іншою назвою – відділ по зв'язках з громадськістю, економічного аналізу або маркетингових досліджень. Найбільшого ефекту вдається досягти, коли підрозділ фінансової розвідки формується внаслідок об'єднання аналітичного відділу та служби безпеки підприємства. Для того щоб максимально ефективно організувати роботу цього підрозділу, при його створенні керівництво компанії має вирішити: яка вимагається інформація; які методи збирання даних допустимі при роботі підрозділу; як організувати зберігання і структурування інформації; хто буде мати доступ до отриманої інформації.

Організація економічної розвідки залежить від характеру і обсягів виробництва та формування стратегічного потенціалу підприємства. Тому визначення заходів щодо запобігання загрозам економічній безпеці підприємств вимагає врахування багатьох факторів і, особливо розмірів фірми та обсягів ресурсів для організації економічної розвідки.

Розвідка в крупних фірмах найчастіше організована у формі холдингової компанії, штаб-квартира якої перебуває подалі від співробітників компанії. Всі

спецслужби великої корпорації поділяються на групи: 1) спецслужба країни базування; 2) спецслужба в зарубіжних країнах.

Основними напрямками роботи спецрозвідок обох груп є: зв'язок з державними розвідками, лобізм в державних і місцевих законодавчих і виконавчих органах влади, безпосередня розвідка конкурента (рис. 4.4).

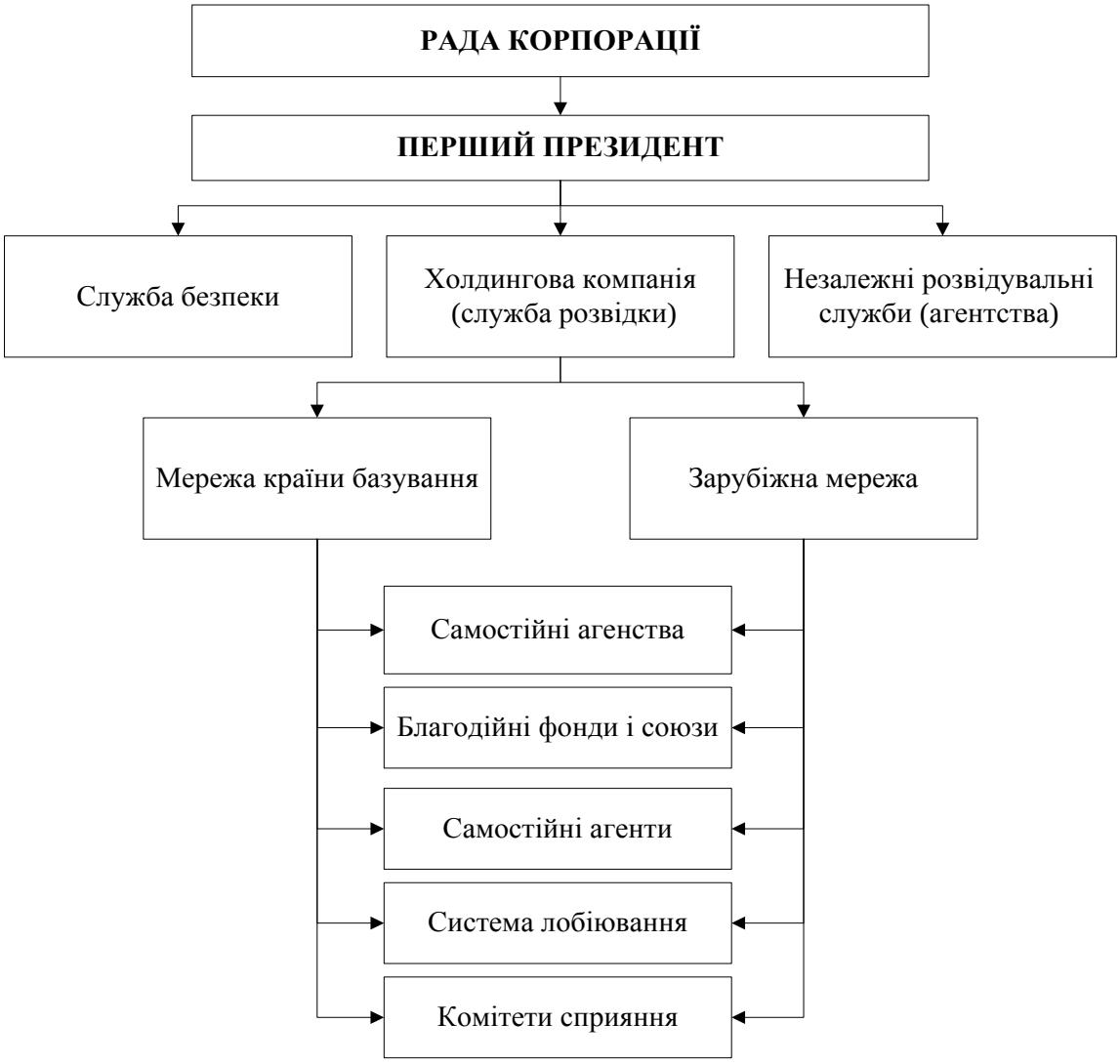

Рис. 4.4. Схема організації економічної розвідки великої фірми

Штаб-квартира розвідслужби та її агентства мають самостійних агентів і резидентів із відповідним підпорядкуванням. До традиційних груп агентів слід увести нову категорію: агент-експерт, який обробляє легальні матеріали, відшуковує необхідну інформацію про економічний стан конкурента.

Особливе місце в організації розвідувальної роботи великого і середнього бізнесу відведено створенню різного роду благодійних фондів і союзів, які забезпечують лобіювання прийняття рішень на всіх рівнях законодавчої і виконавчої влади.

Організація розвідки у середніх фірмах полягає у наступному: організація розвідувальної роботи проводиться вузьким колом людей (в межах кількох

чоловік); до розвідувальної роботи на конфіденційній основі залучаються кваліфіковані спеціалісти фірми; більшою мірою використовуються послуги незалежних агентів і спеціалістів.

Середнє підприємство може мати спеціальний розвідвідділ або групу, про яку знає досить обмежене коло осіб. Підрозділ може бути самостійним або групою будь-якого підрозділу фірми. Він може називатися, наприклад, «відділом дослідження зовнішнього середовища», який організовує економічну розвідку по таких основних напрямках: обробка легальної економічної інформації про конкурентів службовцями фірми; вербування агентів у конкурентів; встановлення контактів із незалежними агентствами і агентами; організація лобі на місцевому рівні.

Особливості організації розвідки малими фірмами. Оскільки малі фірми працюють на вільних, хоча і локальних, ринках, в них на відміну від великих корпорацій і середніх фірм є безліч конкурентів. Об'єктом економічної розвідки для малого підприємства стає ринкова інфраструктура: банки, страхові компанії, збутові і постачальницькі фірми (покупці і постачальники) і т.п., які виступають кредиторами, гарантами, замовниками.

Організатором збирання цієї інформації виступає менеджер малого підприємства. Він може отримувати відомості: від консультантів спеціальних консалтингових фірм, які на основі огляду відкритої інформації роблять відповідні висновки про стан того чи іншого підрозділу ринкової економіки; від працівників підрозділів ринкової інфраструктури, які можуть працювати консультантами у малому підприємстві і за відповідні гонорари надавати необхідну інформацію та поради; від незалежних розвідувальних агентств і агентів; і нарешті, якщо мале підприємство має спонсором велику фірму, - від її служби.

Таким чином, особливості організації економічної розвідки на підприємствах різних типів зводяться до змін співвідношення між зовнішніми і внутрішніми джерелами одержаної інформації. В міру збільшення розмірів підприємства відносно скорочується питома вага інформації, купленої у незалежних розвідувальних агентств, агентів, консалтингових фірм і консультантів, а відповідно зростає значення спеціальних підрозділів корпорацій.

Стратегія організації економічної безпеки підприємства передбачає врахування загроз зовнішнього і внутрішнього середовища. Зовнішнє середовище несе загрози в тому, що постачальник може розірвати договір, а покупець відмовитися від замовлення. Проти фірми недобросовісний конкурент може здійснити диверсію, а майно та інформація можуть бути викрадені.

Внутрішнє середовище несе дві головні загрози: недотримання технологічних режимів (вибух, пожежа, інфекція та інші забруднення середовища) та недотримання режиму роботи організації і режиму комунікації (втрата інформації). В цілому служба безпеки фірми може протиставити цим явищам систему організації по запобіганню можливих загроз.

Суть захисту зводиться до нейтралізації і запобігання загроз, а якщо такі відбуваються, то до відшкодування нанесеної шкоди. Спочатку визначаються об'єкти захисту:

1) інтереси організації (вони визначені її місією, стратегією і цілями). Проявляються у відносинах з державними органами, партнерами, представниками, громадськістю і засобами масової інформації;

2) власність організації, яка слугує одним із провідних засобів досягнення мети і реалізації інтересів. Формою власності є всі економічні ресурси, за винятком персоналу, які належать підприємству: будівлі, споруди, обладнання, готова продукція тощо;

3) інформація як важлива форма власності, яка виступає одним із найважливіших об'єктів захисту в сучасних умовах;

4) технологія – одна із форм власності, охорона якої має принципове значення (ноу-хау, патенти, ліцензії тощо);

5) економічні, кооперативні та інші зв'язки з партнерами. Вони потребують захисту від посягань конкурентів, які завжди прагнуть їх розірвати;

6) продукція і послуги, які поставляються організацією споживачам;

7) транспортні засоби і транспортовані вантажі;

8) персонал, який є носієм інформації.

Наведені об'єкти захисту охороняються різними способами, серед яких як основні можна виділити:

– *юридичний захист,* призваний охороняти законні права фірми і її співробітників у взаємовідносинах з державою, юридичними і фізичними особами;

– *економічний захист* – облік економічних інтересів фірми у взаємовідносинах з державою, фізичними і юридичними особами при оформленні відносин поставок, реалізації продукції, інвестицій і платежів;

– *інформаційний захист* – запобігання втратам секретної інформації;

– *фізичний захист* – припинення дій фізичних осіб, спрямованих на викрадення власності підприємства, спроб нанесення шкоди руйнуванням власності, технологій, комунікацій тощо;

– *соціально-психологічний захист* передбачає проведення виховної роботи у колективі з метою створення атмосфери патріотизму та відданості інтересам фірми.

Основу *стратегії захисту інформації* повинна складати схема комунікаційної системи організації, яка включає чотири елементи: джерело інформації; інформацію, яка виходить із цього джерела; канал, по якому передається інформація; адресат інформації.

Очевидно, що інформація може бути викрадена безпосередньо із джерела, із каналів, по яких вона циркулює (пошта, телефонний зв'язок, радіо і телевізійна та інша електронна мережа), а також у адресата. Отже, першим кроком у захисті інформації є охорона всіх ланок комунікаційного ланцюга, по якому циркулює інформація. Для цього перш за все відокремлюють інформацію, яка є особливим секретом фірми. Вона не повинна циркулювати

по загальній системі. Служба безпеки повинна організовувати не тільки охорону, але й оцінювати секретну інформацію за вартістю створення і придбання та конкурентоспроможністю (можливих вигодах).

Важливою складовою *стратегії гарантування економічної безпеки підприємства* є забезпечення безпеки його персоналу. Інтересам фірми можуть виникати такі загрози: продаж персоналом секретів фірми; вибування персоналу розвідкою конкурента; викрадення провідних спеціалістів фірми; балакучість співробітників; крадіжки майна, грошових засобів персоналом фірми. Служба безпеки фірми повинна здійснювати перевірку благонадійності персоналу, особисту охорону найбільш цінних працівників фірми, проводити виховну роботу і створювати відповідний режим та захист майна і інформації.

Можна виділити такі головні методи перевірки благонадійності персоналу фірми: психофізіологічний і соціометричний.

Психофізіологічний метод доцільно використовувати при відборі кандидатур на роботу, зв'язану з особливо секретною інформацією, збереженням матеріальних цінностей, фінансами. Випробування майбутніх працівників здійснюється на основні тестів, які повинні бути індивідуалізованими, тобто питання мають спиратися на біографічні дані досліджуваного.

В процесі перевірки працюючих спеціалістів доцільніше застосовувати *соціометричні* методи. Суть їх зводиться до того, що потенційна можливість нелояльного відношення до фірми з боку окремих працівників визначається за оцінками колег і товаришів. Можлива ситуація, коли на основі факту витікання секретної інформації ведеться пошук її джерела. Тоді соціометричний метод значно звужує коло пошуку.

Контрольні питання:

1. Розкрийте сутність фінансового моніторингу.
2. Сутність поняття «брудні гроші».
3. Законодавча основа проведення фінансового моніторингу.
4. Завдання, які необхідно виконати при протидії відмивання «брудних грошей».
5. Система заходів запобігання відмивання грошей.
6. Структура системи фінансового моніторингу.
7. Основні завдання фінансового моніторингу
8. Форми організації системи фінансового моніторингу.
9. Підрозділи фінансового розвідки.
10. Зарубіжний досвід використання фінансової розвідки.
11. Класифікація системи фінансового моніторингу.
12. Об'єктивна та суб'єктивна система фінансового моніторингу.
13. Характеристика об'єктивної системи фінансового моніторингу.
14. Суб'єктивна модель фінансового моніторингу та її особливості.
15. Вітчизняна модель фінансового моніторингу.
16. Національна система України по боротьбі з відмивання коштів.

17. Повноваження суб’єктів державного фінансового моніторингу.
18. Джерела інформації при фінансовій розвідці.
19. Чинники, що впливають на ефективність фінансової розвідки.
20. Мета створення служби фінансової розвідки на підприємстві.

Тема 5. *Забезпечення інформаційної безпеки фінансових систем*

План:

5.1 Поняття інформаційної безпеки фінансових систем

5.2 Проблеми забезпечення інформаційної безпеки фінансових систем

5.3 Сучасний стан інформаційного простору в постіндустріальних країнах

5.1 Поняття інформаційної безпеки фінансових систем

Нові реалії сьогодення характеризуються стрімким розвитком інформаційно-телекомунікаційних технологій, інтенсивним впровадженням новітніх інформаційних технологій в усі сфери суспільного життя. Зважаючи на це інформація та новітні інформаційно-телекомунікаційні технології дедалі більше визначають розвиток держави і суспільства, сприяють розвитку інформаційного середовища. Звичайно, ефективне та злагоджене функціонування інформаційного середовища потребує розробки та впровадження низки організаційно-правових заходів, зокрема заходів щодо своєчасної організації функціонування системи інформаційної безпеки. Однією із складових інформаційної безпеки є інформаційна безпека підприємництва в рамках якої має здійснюватися дієвий захист джерел інформації про комерційну діяльність підприємств усіх форм власності, інформаційно-аналітичних систем збору та обробки фінансової, податкової інформації.

Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів тощо. Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації. Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, відповідальних за безпеку інформації; вирішення проблеми керування захистом інформації і її автоматизації; створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організація підготовки відповідних фахівців та ін. Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як: за- хист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни.

Існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку це самостійний елемент національної

безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д. Одним з найбільш повних визначень інформаційної безпеки можна вважати наступне: це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Це визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб'єктів держави. Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Основними складовими останньої є: національна безпека, національні інтереси, національні цілі, пріоритети і принципи задоволення і захисту національних інтересів, загрози національній безпеці і система національної безпеки. Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України».

Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства». Так, Цимбалюк В. характеризує інформаційну безпеку як стан інформації, в якому забезпечується збережен ня визначених політикою безпеки властивостей інформації. Фурашев В. вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створен ня, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності. Гуцу С. пропонує розглядати інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Литвиненко О. під інформаційною безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності. Цікавим та водночас дискусійним є визначення Кормича Б., який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, всього суспільства та держави. Харченко Л., Ліпкан В., Логінов О. визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України. Таким чином, інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних засобів, що є в її розпорядженні. Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних

технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору. Сороківська О. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності. Танцюра М. характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації: доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [8, с. 452]. Поряд з цим, Марущак А. визначає інформаційну безпеку підприємства як цілеспрямовану діяльність його органів та посадових осіб з використанням дозволених сил і засобів щодо досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Завжди існували загрози інформаційній безпеці фінансових систем серед них найбільш небезпечними були такі.

1. Слабка інтегрованість України у світове інформаційне поле, недостатня кваліфікованість й активність її інформаційних служб. Це є причиною того, що уявлення про Україну формують у світовому інформаційному полі не її власні засоби масової інформації, а відповідні засоби та агентства інших держав. При цьому останні виходять із своїх геополітичних, політичних, військових, економічних інтересів. Таким чином, формується спотворений образ України, її зовнішньої та внутрішньої політики, що негативно впливає на її міжнародний авторитет. Крім того, Україна не може протистояти інформаційно-пропагандистським акціям інших держав, які через вторгнення в інформаційний простір України намагаються забезпечити свої політичні та економічні інтереси, що створює загрозу національній безпеці України.

2. Використання засобів масової інформації окремими політичними силами. Для реалізації своїх планів окремі політичні партії, рухи, громадські об'єднання України використовують засоби масової інформації України. З цією метою проводяться пропагандистські кампанії, розповсюджується спеціально підібрана інформація тощо.

3. Негативні наслідки міжпартійних відносин. Деякі політичні партії, рухи, об'єднання у боротьбі за посилення свого впливу, а також з метою реалізації вузькопартійних цілей забувають про необхідність збереження в Україні загальнонаціональної стабільності і злагоди, нехтують чинним законодавством. Це призводить до того, що вони використовують засоби масової інформації, друковану продукцію, наочну агітацію таким чином, що це створює загрозу інформаційній безпеці. Йдеться про нав'язування за допомогою засобів масової інформації певних політичних кліше, а також штучне

загострення ситуації, роздмухування пристрастей, використання погроз, закликів до помсти чи до реваншу, використання однобічної, спеціально відібраної інформації.

4. Вплив міжконфесійних конфліктів. Проблеми і конфлікти, що існують у релігійній сфері, призводять до появи в інформаційному просторі України небезпечних явищ – погроз, нацьковування однієї частини віруючих на іншу, поширення необ'єктивної інформації, яка здатна загострити ситуацію.

5. Некомпетентність працівників державних органів і установ. Цей чинник негативно впливає на якість і спрямованість інформаційного матеріалу і тим самим створює можливість соціально-політичних конфліктів. Його дія виявляється через неповну, запізнілу інформацію.

6. Недостатній професійний рівень працівників засобів масової інформації. У засобах масової інформації, друкованій продукції з'являються матеріали, що пропагують вседозволеність, аморальність, нехтування патріотичними та громадськими обов'язками, моральними принципами. Це може призвести до загострення соціально-економічного та політичного стану.

7. Вплив на засоби масової інформації організованої злочинності, мафіозних структур. Злочинні угруповання намагаються перешкодити розбудові міцної демократичної держави, створити в Україні умови всеохоплюючої корумпованості тощо. З'являється інформаційна продукція, що підриває авторитет і довіру до правоохоронних органів, державних структур, пропагує кримінальний світ.

8. Недосконаліть технічного захисту інформаційного простору України. У зв'язку з тим, що обробка інформації, у тому числі й такої, що становить державну таємницю, здійснюватиметься з використанням найсучасніших технічних засобів, виникає необхідність у її технічному захисті.

5.2 Проблеми забезпечення інформаційної безпеки фінансових систем

Ключовою проблемою інформаційної безпеки є оцінка відповідності існуючого в державі інформаційного простору потребам її громадян, попиту та пропозиції інформаційних послуг у наближених до користувачів місцях та в зручний для них час.

Історичний досвід свідчить, що країни, які не спромоглися своєчасно поповнити національний інформаційний простір більш ефективними технологіями, сповільнювали свій економічний розвиток. І навпаки, країни, що мали потужний інформаційний потенціал швидко відновлювали свою роль у світовому розподілі сфер впливу навіть після воєнних поразок. Тому наповнення національного інформаційного простору новітніми технологіями, що здатні істотно підвищити як адекватність віддзеркалення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що у свою чергу визначає можливості захисту національних інтересів.

Перспективи розвитку України як суверенної держави в першу чергу пов'язані із створенням на її території більш досконалого інформаційного простору порівняно з успадкованим та наданням цьому простору властивостей, які притаманні постіндустріальним країнам.

На жаль, Україна успадкувала від колишнього СРСР переважно транзитні складові загальносоюзної технологічно застарілої інформаційної системи планової економіки і військово-промислового комплексу. Центральні аналітичні компоненти та новітні технологічні елементи, які почали запроваджуватися в СРСР на рубежі 90-х років, залишилися переважно в Російській Федерації.

Аналіз причин недосконалості існуючого в Україні інформаційного простору дає можливість визначити основні з них.

1. Нагальні потреби управління національним виробництвом економічними методами перевищують можливості структурного і змістовного наповнення інформаційного простору.

2. При подоланні інформаційної кризи акценти зроблено не на розвиткові інформаційної периферії, яка повинна реєструвати та зберігати поточні записи у формі, придатній для оперативного використання, а на побудові аналітичних, ситуаційних та інших центрів, призначених споживати, а не створювати інформацію.

3. Національний інформаційний простір не налаштований на реєстрацію фактографічних записів у безпаперовій формі, які віддзеркалюють поточний кількісний вимір властивостей об'єктів.

З'явилася значна кількість нової інформації, наприклад, житлові субсидії, персоніфіковані майнові сертифікати, декларації про доходи громадян, акції підприємств, митне обслуговування кордонів тощо, яка все більше завантажує існуючий інформаційний простір і відволікає значну кількість людей від виробничої сфери. Вона потребує відповідного перерозподілу фінансових та інших ресурсів. Поряд з цим продовжують відтворюватися умови, за яких подальше споживання детальної інформації – продукту їхньої діяльності – може бути організоване лише ієрархічною вертикаллю відповідними посадовими посередниками шляхом виконання великих обсягів рутинних робіт за регламентованими механізмами узагальнення та звітування. На кожному щаблі узагальнення інформація, як правило, зазнає випадкових (або не випадкових) спотворень у приватних чи відомчих інтересах навіть при бездоганній відповідності записів базового рівня подіям реальності. Існуючий в Україні інформаційний простір штучно розділяється на сукупність неузгоджених за семантичними ознаками і технологіями відомчих інформаційних анклавів, які безсистемно нашаровуються. Все це розпорошує ресурси, не забезпечує верифікацію записів базового рівня на засадах інтересів усіх суб'єктів суспільства. Такий стан інформаційного простору фактично робить органи управління вищих рівнів заручниками інформаційної діяльності підлеглих.

Саме з цієї причини аналітичні матеріали, які використовуються при прийнятті рішень, тяжіють до макроекономічних показників або результатів

соціологічних опитувань, що свідчить про ускладнене отримання або повну відсутність детальних записів у деяких сегментах економіки держави.

Проблематичним також є те, що Україна успадкувала адміністративно-командні методи створення інформаційних систем, які спиралися на розгалужену систему наукових, конструкторських і виробничих установ, що працювали практично поза конкуренцією, переважно на військово-промисловий комплекс, при відносно сталому задовільному бюджетному фінансуванні. З іншого боку, схема фінансування наукоємних виробництв, до яких належить інформаційна сфера, практично залишилася без змін, за винятком істотного скорочення обсягів фінансування до рівня, який сьогодні не забезпечує навіть функції соціальної допомоги.

Аналіз ряду концепцій інформатизації, проектів, структур міністерств та відомств свідчить, що навіть у свідомості фахівців переважає адміністративно-командне мислення, яке втілюється в численних пропозиціях щодо запровадження в Україні різноманітних ситуаційних, аналітичних, інформаційних, оперативних та інших «центрів». Водночас необхідність побудови периферійної системи створення і зберігання інформаційних ресурсів як середовища для об'єктивного і структурованого віддзеркалення подій і явищ на місцях, що призначене для модернізації існуючого переважно паперового інформаційного простору, або не розглядається взагалі, або вважається передчасною.

Делікатною проблемою є використання закордонних кредитів для розвитку інформаційних технологій. Як свідчить аналіз тендерних документів, зазначені кредити використовуються переважно для імпорту комп'ютерів та іншого обладнання обчислювальної та офісної техніки. Водночас відомо, що строк морального старіння такого обладнання досить стислий і не перевищує нині трьох-п'яти років. Науково-технічний прогрес унеможливлює використання сучасних інформаційних технологій вже через п'ять років. Тому від інвестицій на час їхнього повернення з відповідними відсотками Україна матиме борги, а не закуплену техніку. Існуюча практика укладання контрактів із зарубіжними фірмами – постачальниками технологій – призводить до використання кредитів на найпростіші цілі – закупівлю та монтаж обладнання, меблів, переобладнання приміщень тощо. Як результат – підтримка закордонних виробників за рахунок отриманих кредитів. Поряд з цим довгострокові і набагато складніші процеси створення інформаційних ресурсів, розв'язання прикладних задач, впровадження інформаційних технологій, тобто ті справи, заради яких закуповується обладнання, залишаються фактично без фінансування, хоча відомо, що саме вони потребують коштів на порядок більших, ніж вартість обладнання та програм загальносистемного призначення.

Визначення загальних засад створення сучасної державної інформаційної системи, яка б функціонально відповідала ринковим потребам, залишається складною проблемою.

Тяжкою спадщиною тоталітарного минулого для України є закритість об'єктивної інформації для широкого загалу. З одного боку, ця закритість є

природним наслідком нерозвиненості національного інформаційного простору, а з іншого – її причиною є відомча "приватизація" даних, яка робиться під гаслом захисту державної або комерційної таємниці, звужуючи проблему інформаційної безпеки держави до окремих її аспектів.

Концептуальні засади захисту інформації потребують перегляду передусім з точки зору економічної доцільності. Головним методом захисту важливої інформації має бути не запровадження загальних переліків відомостей, які становлять державну таємницю, а конкретна інформаційна контргра щодо намірів, а не результатів їхнього втілення. Ця контргра має вестися на зразок різних суперечливих інформаційних повідомлень (тобто дезінформація), оскільки важливу для національної безпеки інформацію неможливо захистити загальними засобами.

Необхідною умовою ведення сучасної інформаційної боротьби є наявність сучасного потужного інформаційного простору в державі. Інформаційний захист національних інтересів повинен концептуально розглядатись як динамічний процес.

Головним носієм інформації завжди була і є людина, свобода пересування якої є природним правом у демократичних державах. Тому методи захисту інформації повинні виходити з цієї парадигми, а не копіюватись механічно з тоталітарного минулого.

Потребують істотного вдосконалення механізми реєстрації інформації, що отримується Україною в результаті її міжнародної діяльності. Аналіз інформаційних аспектів міжнародних договорів, які ратифіковані або парафовані Україною, зокрема Договору про безпеку і співробітництво в Європі, Договору «Відкрите небо», Угоди про партнерство та співробітництво між Європейським співтовариством і Україною, Додаткового протоколу до Європейської конвенції про інформацію щодо іноземного законодавства та інших міжнародних угод, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах. Необхідно поступово відходити від стану інформаційного донорства і переходити до інформаційного партнерства. Складовою такого механізму повинна бути система сучасних національних архівів-депозитаріїв для зберігання та споживання інформації, що отримується Україною від інших країн на виконання зазначених угод, та поширення в державі механізмів доступу до інформаційних баз даних за кордоном.

Потребують істотного доопрацювання механізми профільного накопичення та зберігання інформації в структурах державного управління. Треба створити такі інформаційні умови, щоб при підготовці важливих нарад, засідань Уряду, Верховної Ради, Ради національної безпеки і оборони України тощо добір необхідної інформації здійснювався не «пожежними» заходами з використанням одноканальних джерел інформації, яку неможливо перевірити.

Зміст, порядок реалізації забезпечення інформаційної безпеки, інструменти, завдання та нормативне регулювання цього процесу полягають у наступному:

1. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері.

2. Інструментом реалізації державної політики інформаційної безпеки виступає система забезпечення інформаційної безпеки. Остання представляє собою організаційне поєднання заходів (інформаційного, адміністративного, управлінського, методологічного характеру), спрямованих на забезпечення інформаційної безпеки особистості, суспільства і держави.

3. Завданнями системи забезпечення інформаційної безпеки є:

– моніторинг, прогнозування реалізації дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави;

– здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

– створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки;

– вдосконалення державної політики розвитку інформаційної сфери (створення сприятливих умов розвитку національної інформаційної інфраструктури, впровадження новітніх технологій у цій сфері);

– забезпечення інформаційно-аналітичного потенціалу країни.

4. Нормативно-правове регулювання системи забезпечення інформаційної безпеки України представлено: Конституцією України, Законом України «Про основи національної безпеки України», Законом України «Про інформацію», Законом України «Про Концепцію Національної програми інформатизації», Указом Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі», іншими актами.

5. Органами забезпечення інформаційної безпеки виступають органи законодавчої, виконавчої і судової влади, а також служби (органи) захисту інформації підприємств, організацій, установ: Президент України (в межах своїх повноважень, здійснює керівництво у сфері інформаційної безпеки);

– Національний інститут стратегічних досліджень (координує наукові дослідження з питань інформаційної безпеки);

– Рада національної безпеки і оборони (РНБО) України (координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки);

– Кабінет Міністрів України (забезпечує здійснення внутрішньої та зовнішньої політики, виконання Конституції і законів України, актів Президента України в інформаційній сфері; вживає заходів щодо забезпечення прав і свобод громадян, забезпечення інформаційної безпеки України, боротьби зі злочинністю в інформаційній сфері; під час формування проекту бюджету передбачає виділення необхідних коштів для виконання загальнодержавних програм, спрямованих на забезпечення інформаційної безпеки України);

– Державний комітет телебачення і радіомовлення України (вносить пропозиції щодо формування державної політики в інформаційній та видавничій сферах, забезпечує її реалізацію, здійснює управління в цих сферах, міжгалузеву координацію та функціональне управління; здійснює координацію діяльності державних засобів масової інформації; аналізує і прогнозує тенденції розвитку інформаційного простору України, здійснює заходи щодо його захисту);

– Національна Рада України з питань телебачення і радіомовлення (вирішує питання: забезпечення свободи слова та масової інформації; прав телеглядачів і радіослухачів, виробників і розповсюджувачів масової звукової, візуальної та аудіовізуальної інформації);

– Конституційний Суд України (вирішує питання про відповідність законів та інших правових актів в інформаційній сфері Конституції України, дає офіційне тлумачення Конституції та законів України з відповідних питань);

– Держстандарт (розробляє стандарти в області захисту інформації);

– органи СБУ (виконують функції захисту державної таємниці);

– органи МВС (ведуть боротьбу з правопорушниками в інформаційній сфері і комп'ютерними злочинами. Для цього в структурі МВС створено спеціальне управління для запобігання і розкриття комп'ютерних злочинів і захисту авторських прав);

– органи Державного митного комітету (попереджають незаконне ввезення і вивіз з України «піратської» продукції, забезпечуючи тим самим захист авторських і патентних прав).

6. Перелік функцій системи забезпечення інформаційної безпеки України: удосконалення нормативно-правового поля регулювання розвитку інформаційних ресурсів; оптимізація державної політики інформатизації; регулювання інформаційного співробітництва; контроль за встановленим порядком і правилами формування і використання інформаційних ресурсів [4, 6].

Отже, інформаційна безпека має одне з першочергових значень для соціально-економічного розвитку держави. Україна має продовжити активні кроки на шляху розбудови власної системи інформаційної безпеки.

Важливими заходами в цьому процесі мають стати організація і проведення інформаційних операцій, а також розвиток системи сертифікації інформаційних продуктів. Окрім того, система забезпечення інформаційної безпеки повинна гнучко коригуватися відповідно до мінливого характеру зовнішніх та внутрішніх факторів оточення

5.3 Сучасний стан інформаційного простору в постіндустріальних країнах.

Інформаційна система держав з ринковою економікою істотно відрізняється від наведеної вище схеми. Її функцією є обслуговування ринку, тобто забезпечення механізму зв'язування попиту та пропозиції, покупців і продавців, реєстрація актів купівлі й продажу, запобігання недобросовісній

конкуренції, захист прав споживачів, здійснення державного контролю за критичними для національної безпеки галузями виробництва, забезпечення конкурентоспроможності вітчизняних товарів на внутрішньому і зовнішніх ринках тощо. Головним призначенням такої системи є забезпечення доцільності тієї чи іншої виробничої діяльності через критерій максимального прибутку кожної окремої виробничої або посередницької одиниці. Система обслуговує втрату власності у разі неефективного її використання. Така інформаційна система набагато складніша і відкритіша, ніж ієрархічна система планової економіки.

Слід зауважити, що ті чи інші інформаційні системи завжди існували для обслуговування ринкових відносин, але країни, що посіли чільне місце серед постіндустріальних, створили більш ефективну інформаційну ситуацію завдяки подвійній дії концептуальних принципів відкритості інформації та запровадження новітніх досягнень науково-технічного прогресу. Це дало змогу утворити інформаційний простір, який оперативніше віддзеркалює на широкий загал різні події: ціни на товари та послуги, курси валют, вартість дорогоцінних металів, наявність ресурсів та інші дані, що необхідні для прийняття виважених рішень.

Важливою обставиною є те, що механізм споживання інформації налаштовано на ініціативу абонента. Поряд з цим механізми створення і зберігання інформаційних ресурсів орієнтовано на їхнє відторгнення від кореспондента. Релевантне запитам споживання інформації здійснюється без переміщення споживача до місця її зберігання, наприклад бібліотеки або картинної галереї, і без залучення інших посередників, оскільки інформаційна система є інтегруючим посередником кожного з кожним.

Характерною ознакою інформаційної досконалості постіндустріальних країн є витіснення національної готівки у країни з менш досконалим інформаційним станом і, як результат, нееквівалентний обмін товарами і послугами. Водночас пріоритетними напрямками інформаційної діяльності на внутрішньому ринку є антимонопольна протидія, національне заощадження невідтворюваних ресурсів (передусім енергетичних та екологічних), постійна структурна перебудова ринку праці і відповідний життєвий рівень громадян, які створюють і споживають інформацію.

Створення інформаційних технологій є одним з найбільш розвинених, динамічних, прибуткових й експансивних секторів економіки постіндустріальних країн.

Таким чином, головним призначенням інформаційних систем у цих країнах є забезпечення постійної і масової дії мікроекономічних механізмів від'ємного зворотного зв'язку через конкурентне змагання за найбільший особистий чи корпоративний прибуток. А головним наслідком є макроекономічна стабільність системи і водночас її оперативна чутливість до науково-технічного прогресу.

Сьогодні неможливо уявити інформаційний простір без комп'ютерної мережі. Саме ці технології дали поштовх виникненню та розвиткові багатьох

видів бізнесу: електронним розрахунковим карткам, оперативним міжбанківським розрахункам, обслуговуванню бірж, брокерським конторам тощо.

З огляду на функціональне призначення інформації вирішуються питання безпеки і технологій її створення та споживання. Відповідним чином розробляються принципи безпеки, на яких базуються нові технології та обслуговування інформаційних ресурсів.

Без новітньої надбудови національного інформаційного простору історичні перспективи суверенного існування України досить примарні. Практичне здійснення технологічної надбудови національного інформаційного простору вимагає визначеності у таких питаннях: що реєструвати у вигляді записів, як реєструвати, де і як зберігати, де і як споживати, як верифікувати адекватність і повноту інформації. Ключовим із зазначених є питання зберігання інформації, оскільки відповіді на інші питання залежать від механізмів його вирішення.

Сьогодні передовий досвід побудови систем управління ґрунтується на використанні процесного підходу. Сенс його полягає в безперервному поліпшенні системи захисту через переоцінку ризиків, аналіз, постійне вдосконалення моделей захисту і забезпечення безперервності бізнесу.

Таким чином, система управління інформаційною безпекою повинна включати процедури аналізу і переоцінки ризиків, порівняння показників по періодах і внесення відповідних змін до процедури забезпечення інформаційної безпеки.

Зокрема, періодичної оцінки повинні підлягати наступні позиції:

– стан інформаційної системи, визначення номенклатури інформаційних ресурсів та правила їх об'єднання в робочі групи;

– категорії даних, що обробляються інформаційною системою, матеріальна оцінка збитку в разі дискредитації даних;

– організація роботи користувачів інформаційної системи, визначення приналежності груп користувачів до певних інформаційних ресурсів, види і права доступу до інформації, визначення режиму доступності інформації (час простою при спробі доступу до інформації в кожній з груп користувачів);

– опис бізнес-процесів та їх прив'язки до інформаційних ресурсів і категоріям оброблюваної інформації;

– ефективність організаційних заходів захисту інформації, організація фізичного захисту доступу до інформаційних ресурсів, захист робочих місць, безпеку персоналу, управління комунікаціями і процесами, процедури контролю доступу, можливість внесення змін в виконувані файли і бібліотеки інформаційних ресурсів, функціонування та актуальність плану забезпечення безперервності бізнесу, відповідність документованим вимогам політики безпеки.

Наступним кроком в управлінні ризиками бачиться перехід до інтегрованої системи менеджменту (ІСМ).

Система ґрунтується на гармонізації різних систем управління (IT, інформаційною безпекою, якістю, фізичної безпекою, забезпеченням безперебійної роботи ключових сервісів) і впровадженні інтегрованого підходу до управління ризиками.

Традиційно ризики оцінюються на рівні активів (IT-ресурси, персонал, репутація, чутливі дані), і карта ризиків заповнюється з точки зору інформаційної безпеки. ІСМ пропонує розширити область оцінки і розглядати активи як ризикоутворюючі фактори для цілого набору систем управління. Таким чином, карта ризиків доповнюється відомостями і з боку інших систем управління.

Міграція в сторону ІСМ на базі процесного управління дозволяє розглядати ризики безпеки підприємницьких структур з урахуванням усіх аспектів діяльності. ІСМ, безсумнівно, буде служити подальшому розвитку якості роботи профільних підрозділів банків.

Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей. У першій частині статті 17 Конституції України забезпечення інформаційної безпеки України проголошено «справою всього українського народу».

Ефективність системи забезпечення інформаційної безпеки держави стає вирішальним чинником в політиці будь-якого суб'єкта геополітичної конкуренції. Неефективність системи інформаційної безпеки може стати чинником, здатним привести до великомасштабних аварій і катастроф, наслідки яких можуть викликати, зокрема, дезорганізацію державного управління, крах національної фінансової системи тощо.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Основними напрямами забезпечення інформаційної безпеки є:

– у сфері міжнародної співпраці – інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця по запобіганню протиправних дій в інформаційній сфері;

– у сфері оборони – вдосконалення системи моніторингу загроз та їх джерел, своєчасне інформування відповідних суб'єктів влади про стан інформаційного ресурсу і інформаційних систем оборонної сфери; засобів, методів і способів здійснення, спеціальних заходів і заходів інформаційного впливу;

– системи підбору і спеціальної підготовки користувачів.

В Україні проводиться послідовна робота з розбудови інформаційного суспільства. 29 серпня 2012 року Кабінет Міністрів України схвалив проект Указу Президента України «Про Стратегію розвитку інформаційного

суспільства в Україні». У Стратегії відображені принципи, базові для інформаційного суспільства – це партнерство влади, суспільства і бізнесу, а також відкритість, відповідальність та ефективність самої влади. Реалізувавши Стратегію, Україна стане рівноправним учасником глобального інформаційного суспільства.

В умовах формування глобального інформаційного суспільства в сучасних конфліктах з'явилася нова фаза – інформаційно-психологічна війна, яка займає проміжну сходинку між політичною кризою і фазою збройного зіткнення, будучи при цьому «поворотною точкою» від мирної фази до військової. У цій фазі технології інформаційно-психологічного впливу на політичні (в тому числі, міжнародні) конфлікти стають одним з вирішальних чинників і високоефективних інструментів в діяльності по їх політичному вирішенню.

Сучасні характеристики конфліктів є такими:

– інформаційні війни є першою, часто визначальною, стадією конфлікту;

– на зміну конфліктам з протистоянням держав приходять змішані конфлікти (де сторонами виступають не окремі держави, а коаліції держав, воєнно-політичні блоки);

– війни протікають як спецоперації – не проводиться загальна мобілізація, на перше місце виходить значення військово-повітряних сил, розвідки та високоточної зброї;

– воєнним діям властиві динамічність та короткий термін;

– змінюються приводи до війни (відсутність демократії, конфлікти населення з владою тощо);

– держави, які не мають підготовлених до ведення сучасних воєнних дій збройних сил та сучасних систем озброєння втрачають суверенітет, ресурси тощо.

Основними шляхами запобігання виникненню воєнних конфліктів є:

– забезпечення інформаційної безпеки;

– зміцнення позитивного іміджу України на міжнародній арені шляхом активізації інформаційно-роз'яснювальної роботи з питань воєнної політики держави тощо.

Загрози в інформаційній сфері тісно переплітаються з інформаційною безпекою держави. Аналіз сучасного стану і тенденцій розвитку інформаційного простору України свідчить, що рівень інформаційної безпеки, за окремими показниками, наближається до критично низької межі, за якою може настати втрата демократичних принципів і норм, повернення до авторитаризму, міжнародна ізоляція України.

В сучасних умовах Україні варто зосередитись на двох основних ідеях:

– зробити внутрішній український інформаційний простір сучасним та конкурентоспроможним;

– забезпечити інформаційну присутність держави в світі та просувати позитивний імідж держави за кордоном, а також – що особливо важливо – розробити механізми втілення цього в життя.

Розвиток інформаційного суспільства України та однієї з його складових – електронного урядування, є сучасною глобальною тенденцією, яка веде до істотних змін у суспільних відносинах та економіці країни, що вимагає низки соціально-політичних рішень, які відповідають трансформаціям в усіх сферах життєдіяльності, зокрема, в процесах підготовки та прийняття рішень, в змісті та формах державного управління, в уявленнях про права людини, національну та особисту безпеку, в оцінюванні стратегічних ресурсів. Нині, система електронного урядування і система інформаційної безпеки держави є взаємопов'язаними елементами загальної системи державного управління. Розвиток та впровадження в різні сфери життя суспільства новітніх інформаційних технологій, як і будь-яких інших науково-технічних досягнень, не тільки забезпечує комфортність, але й нерідко несе певну небезпеку.

Зокрема загальними є групи інформаційно-технічних небезпек:

– новий клас соціальних злочинів направлений проти особистості, суспільства, держави, заснований у використанні сучасної інформаційної технології (кібертероризм і кіберзлочинність: махінації з електронними грошима, комп'ютерне хуліганство та інші);

– використання нових інформаційних технологій в політичних цілях;

– електронний контроль за життям, планами громадян, політичних організацій;

– бурхливий розвиток нового класу зброї - інформаційної, яка здатна ефективно впливати на психіку та свідомість людей, на інформаційно-технічну інфраструктуру суспільства і армії.

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері, стабільності в суспільстві є:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії, комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Розвиток інформаційної інфраструктури держави, створення і впровадження нових інформаційних технологій спричиняє за собою не стільки усунення існуючих загроз, скільки виникненню нових. Так наприклад, згідно з новою Воєнною доктриною наша держава вважає військовою загрозою «економічну чи інформаційну блокаду України» та «застосування політичних та економічних санкцій проти України». У контексті ж подій що розгортаються

останнім часом, коли в європейських ЗМІ та європейськими політиками і чиновниками, створюється негативний образ України, а в Євросоюзі та інших міжнародних організаціях активно обговорюють можливі політичні та економічні санкції проти України, цей постулат виглядає незрозумілим, адже якщо ЄС або інші міжнародні організації введуть санкції проти України, то вони автоматично можуть потрапити у розряд потенційних військових супротивників України.

Сучасний глобальний інформаційний простір, в якому одне з провідних місць займає мережа Інтернет, а в цілому засоби масової комунікації, – це віртуальний, несприйманний свідомістю людини світ, керований інформацією. Як зазначив німецький експерт Ральф Бендрат: «Основи «мережевої війни» сьогодні більше, ніж що-небудь віддалені від уявлень, що досі мали місце, про війну і мир. Ця модель, при якій вже не тіло супротивника є об'єктом фізичної атаки, але його воля безпосередньо змінюється шляхом завоювання інформаційного панування, приведе у результаті до того, що будь-яка форма ідеологічного або політичного протистояння оцінюватиметься як війна».

Головним простором війн минулих століть була земля, а у XX столітті велике значення мали вода і повітря. Бойовий простір сучасних і майбутніх війн XXI століття – це передусім ноосфера, розум людини і плоди її інтелектуальної діяльності. В сучасних умовах під консцієнтальною війною (війною на поразку свідомості) людство розуміє війну психологічну за формою, цивілізаційну за змістом та інформаційну за коштами, в якій об'єктом руйнування та перетворення є ціннісні установки народонаселення супротивника, в результаті чого первинні цілі замінюються вторинними, і нижчими за рівнем, з дещо дедалі більшою ймовірністю їх досягнення, причому ця вірогідність, за рахунок економічних та інших матеріальних важелів впливу коливається таким чином, що досягнення зміни цілей сприймається людиною як її благо. Розвиток світової спільноти наочно демонструє, що найважливішим чинником, що визначає розвиток сучасного суспільства, є бурхливі процеси впровадження інформаційних та комунікаційних технологій в усі сфери сучасного життя.

Таким чином, стрімкий розвиток сучасних інформаційно-комунікативних технологій і перехід людства (насамперед, найбільш розвинених країн), що намітився, до глобального інформаційного суспільства, як і будь-яке інше досягнення науково-технічного прогресу, несе в собі не тільки нові блага, але й нові ризики, виклики та загрози.

Кіберзлочинність сьогодні не має державних кордонів, – отже, і зусилля з протидії їй – справа не однієї держави. Можливості загальної комп'ютеризації і всесвітньої павутини Інтернет активно використовуються нелегальними торговцями зброєю, наркоділками, кіберзлочинцями, авторами та розповсюджувачами порнографії, інформаційні війни та кібератаки в міждержавних конфліктах стають все більш небезпечними, ніж застосування традиційних видів зброї.

У сучасних умовах активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують

інформаційні технології для реалізації своїх намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної безпеки держави. Ці та інші фактори сьогодні актуалізують необхідність врегулювання питань інформаційної безпеки на міждержавному рівні через створення відповідної нормативно-правової бази. Проте, вже перші спроби такого роду наштовхнулися на складність і неоднозначність тлумачення різними державами базових політичних і гуманітарних категорій, а також корінні розбіжності в прийнятих ними системах цінностей, що істотно ускладнює пошук спільної мови. Україна в вирішенні даного питання має поки що пасивно-вичікувальний характер через те, що в силу різних причин нашу державу поки що в повному обсязі не влаштовує жоден із запропонованих документів у сфері інформаційної безпеки. Тим не менш, в середовищі українських експертів вже висловлювалася ідея, що Україна могла б скористатися своїм шансом головування в ОБСЄ в 2013 році і запропонувати власний проект всеосяжного документа з міжнародної інформаційної безпеки, для подальшого сприяння зближенню позицій нашої держави з одного боку із Заходом, з іншого – Москвою і Пекіном. Тому, для вирішення даних питань необхідне плідне міжнародне співробітництво багатьох держав світу, як на державному рівні, так і на рівні співпраці між урядовими організаціями та представниками бізнесу у сфері розповсюдження ІТ-технологій.

Зменшення якісних параметрів інформаційних ресурсів України ускладнює ухвалення найважливіших політичних і економічних рішень і при виробленні державної політики призводить до підриву авторитету органів державної влади в суспільстві та на міжнародній арені, порушення функціонування системи державного управління і контролю техногенно-небезпечних об’єктів, систем управління військами тощо. Відстати від цих тенденцій – значить заздалегідь поставити державу і суспільство як сьогодні так і у майбутньому в уразливе положення.

Контрольні питання:

1. Сутність інформаційної безпеки фінансових систем.
2. Назвіть різні підходи до трактування поняття «інформаційна безпека».
3. Найбільші загрози інформаційної безпеки.
4. Проблеми забезпечення інформаційної безпеки фінансових систем.
5. Сучасний стан інформаційного простору постіндустріальних країн.
6. Застосування інформаційних систем в інформаційній безпеці.
7. Послідовність оцінки інформаційної безпеки фінансових систем.
8. Сутність інтегрованої системи менеджменту.
9. Напрямки забезпечення інформаційної безпеки.
10. Характеристика конфліктів сучасності.
11. Шляхи запобігання конфліктів.
12. Сутність інформаційно-технічних проблем.
13. Основні реальні та потенційні загрози інформаційної безпеки в Україні.

14.Сутність кібербезпечності.

15. Тероризм – як одна з загроз інформаційної безпеки сучасного світу.

16. Порядок реалізації забезпечення інформаційної безпеки.

17. Інструменти реалізації забезпечення інформаційної безпеки.

18. Завдання реалізації забезпечення інформаційної безпеки.

19. Напрямки регулювання процесу реалізації забезпечення інформаційної безпеки.

20. Органи забезпечення інформаційної безпеки в Україні

Тема 6. *Система управління діяльністю з аналітичного забезпечення функціонування системи фінансово-економічної безпеки*

План:

6.1 Мета й основні завдання інформаційного забезпечення фінансово-економічної безпеки

6.2 Особливості управління системою фінансово-економічної безпеки підприємства

6.3 Формування системи обліково-аналітичного забезпечення фінансово-економічної безпеки підприємства

6.1 Мета й основні завдання інформаційного забезпечення фінансово-економічної безпеки

Фінансово-економічна безпека є динамічною ознакою, що змінюється під впливом чинників і загроз внутрішнього та зовнішнього середовища. Формування надійної системи фінансово-економічної безпеки підприємства забезпечує його стабільне функціонування і створює умови для зростання його економічного потенціалу.

Головною метою забезпечення фінансово-економічної безпеки підприємства є досягнення стабільності його функціонування та створення умов для подальшого фінансово-економічного розвитку шляхом попередження внутрішніх і зовнішніх загроз.

Основними цілями фінансово-економічної безпеки на підприємстві є такі:

– забезпечення високої фінансової ефективності роботи підприємства;

– підтримка фінансової стійкості та незалежності підприємства;

– досягнення високої конкурентоспроможності;

– забезпечення високої ліквідності активів; – підтримка належного рівня ділової активності;

– забезпечення захисту інформаційного поля і комерційної таємниці;

– ефективну організація безпеки капіталу та майна підприємства, а також його комерційних інтересів.

Фінансово-економічна безпека на підприємстві повинна мати комплексний, системний характер і складатися із взаємопов'язаних організаційно-правових заходів, що здійснюються спеціальними службами, підрозділами підприємства. Такі заходи спрямовані на захист життєво важливих інтересів працівників підприємства від реальних або потенційних загроз для забезпечення успішного фінансово-економічного розвитку самого підприємства.

До основних завдань фінансово-економічної безпеки підприємства відносять:

1. Забезпечення економічної ефективності господарської підприємства, його фінансової стабільності та фінансової незалежності.

2. Захист співробітників суб'єкта підприємницької діяльності, його капіталу, майна, законних прав та комерційних інтересів від протиправних посягань з боку конкурентів і кримінальних угруповань.

3. Збір та аналіз інформації для опрацювання ефективних й дієвих управлінських рішень з питань стратегії і тактики розвитку системи економічної безпеки підприємства.

4. Забезпечення високої конкурентоздатності продукції, товарів та послуг на основі запровадження ефективного управління на підприємстві.

5. Збір, аналіз та оцінка інформації про партнерів, конкурентів, клієнтів, інших фізичних та юридичних осіб, з метою прийняття превентивних заходів і попередження реальних та можливих загроз економічній безпеці;

6. Забезпечення збереження матеріальних цінностей, грошових коштів та відомостей, що становлять комерційну, банківську та іншу таємницю підприємства, що охороняється законом.

7. Організація навчання персоналу підприємства та контролю щодо дотримання ним відповідних вимог, норм та правил, спрямованих на забезпечення економічної безпеки.

8. Розробка інструкції про допуск персоналу фірми до роботи з документами, що містять комерційну, банківську чи іншу таємницю, що охороняється законом, організація ведення закритого діловодства; 9. Інші завдання, спрямовані на забезпечення економічної безпеки підприємства та його сталий розвиток.

Склад і структура системи фінансово-економічної безпеки підприємства залежать від виду його діяльності, організаційно-правової форми власності, масштабів діяльності, ступеню використання нових технологій. Тобто при побудові системи фінансово-економічної безпеки на підприємстві слід враховувати специфіку його діяльності та загрози його нормальному функціонуванню і розвитку.

Таким чином, питання забезпечення фінансово-економічної безпеки підприємств є досить актуальним в сучасних умовах господарювання, так як останнім часом все частішими стають випадки недобросовісної конкуренції, фіктивного підприємництва, рейдерських атак, промислового шпіонажу, які є загрозою нормальному функціонуванню і розвитку вітчизняних підприємств.

Катастрофічні наслідки глобальної фінансової кризи, які нині відчувають фінансові посередники в Україні, багато у чому пояснюються відсутністю або недосконалістю систем їх економічної безпеки, що не змогли забезпечити надійний захист корпоративних ресурсів суб’єктів господарювання від негативного впливу зовнішніх та внутрішніх загроз.

В організації ефективної комплексної системи економічної безпеки не останнє місце займає її інформаційна підсистема, метою якої є формування достатньої сукупності матеріалів та відомостей щодо середовища функціонування установи або організації та їх якісна аналітична обробка та захист від пошкодження, викрадення, деформації, втрати з метою отримання

достовірних даних, необхідних для прийняття ефективних управлінських рішень.

Загалом, інформаційно-аналітичне забезпечення безпеки підприємництва – це вид інформаційно-аналітичного забезпечення підприємницької діяльності шляхом добування, обробки і надання керівництву необхідної інформації.

Головна мета аналітичного забезпечення функціонування системи фінансово-економічної безпеки – це своєчасне викриття на ранній стадії заходів безпосередньої підготовки певних сил для нанесення економічних збитків підприємству, установі або організації та забезпечення відповідних їм дій, а також добування необхідної інформації для планування, підготовки і проведення заходів з метою недопущення можливих дій.

Інформаційно-аналітична робота в організації виконується з метою виявлення схем недобросовісної конкуренції, шахрайства, обману у сфері бізнесу, задля використання їх для виключення потрапляння власної організації у ситуації некерованого ризику.

Інформаційно-аналітичне забезпечення є підґрунтям для формування інформаційної безпеки фінансового посередника.

Таким чином, приходимо до висновку, що інформаційно-аналітичне забезпечення є необхідною ланкою у механізмі формування ефективної системи економічної безпеки суб’єкта господарювання.

Нині не існує наукового визначення поняття інформаційної безпеки фінансового посередника. Дамо авторську характеристику даного терміну, узявши за основу категорію інформаційної безпеки на макрорівні.

Інформаційна безпека – це такий стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність і недостовірність інформації,через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Таким чином, інформаційна безпека підприємств може бути визначена як такий стан його інформаційно-аналітичного забезпечення, що здатний мінімізувати вплив зовнішніх та внутрішніх загроз на результати діяльності установи або організації, нівелювати ризик втрати фінансовими посередниками господарської стабільності та створити умови для їх сталого розвитку.

Проблеми інформаційної безпеки можна поділити на два класи: захист інформації (запобігання загроз інформації); захист від інформації (запобігання інформаційним загрозам).

На нормальний стан інформаційно-аналітичного забезпечення діяльності вітчизняних фінансових посередників, можуть мати вплив:

– дезінформація;
– знищення інформації;
– перекручення інформації;
– підміна інформації;
– підробка інформації;

– блокування інформації;
– копіювання інформації;
– несанкціонований витік інформації;
– несанкціонований доступ до інформації;
– порушення встановленого порядку маршрутизації інформації;
– викрадення інформації;
– модифікація інформації;
– невірне трактування інформації;
– недостовірність інформації;
– недостатність інформації.

Таким чином, справедливим буде визначення інформаційної безпеки як здатності системи протягом заданого періоду часу протистояти несанкціонованому зняттю і модифікації інформації (під несанкціонованим зняттям розуміємо отримання інформації, до якої абонент не має доступу, тобто порушення правил доступу, а під несанкціонованою модифікацією – зміну інформації, котра призводить до порушення її цілісності, яка у даному випадку розуміється не лише як отримана інформація, але й як її повнота).

Надходження та використання інформації у процесі діяльності фінансового посередника відбувається за наступним алгоритмом: від джерела інформації, що може мати внутрішню або зовнішню природу походження, інформація потрапляє до суб'єкта передачі інформації, який направляє її до суб'єкта отримання інформації (у даному випадку фінансового аналітика), завданням якого є інтерпретація інформації, її аналіз та формування із розрізнених відомостей достовірних даних та передача їх до кінцевого користувача, що на основі одержаних даних прийматиме рішення щодо відповідного аспекту діяльності фінансового посередника. Саме на етапі аналітичної обробки інформації існує найбільший ризик її викривлення та спотворення, оскільки технічні засоби, за допомогою яких проводитиметься обробка матеріалів, можуть спрацювати некоректно, а особа, що займатиметься їх діагностикою, здатна надавати суб'єктивне трактування об'єктивної суті інформації, демонструвати особисте ставлення до неї, що неминуче призведе до небезпеки її помилкової інтерпретації. Відповідно, виникає загроза прийняття кінцевим користувачем (адресатом) неправильного господарського рішення, що матиме негативний вплив на рівень економічної безпеки фінансового посередника.

Джерелами інформації, збір і аналіз якої необхідні для забезпечення інформаційної безпеки підприємства, можуть бути:

– різні офіційні джерела (офіційні видання, звіти та документи державних чи інших органів і організацій), що містять відкриту офіційну інформацію;

– неофіційні джерела, що містять більш-менш достовірну усну чи іншу нетаємну інформацію, що одержується з неформальних контактів із носіями даної інформації;

– конфіденційна інформація, що отримується співробітниками шляхом несанкціонованого доступу до цієї інформації;

– внутрішня інформація, що стосується всіх аспектів діяльності.

Шляхи отримання інформації у сфері діяльності фінансових посередникі в можуть бути наступними:

– збір інформації, що міститься в засобах масової інформації, включаюч и офіційні документи,наприклад, судові звіти;

– використання відомостей, поширюваних службовцями конкуруючих фірм;

– біржові документи і звіти консультантів;

– фінансові звіти і документи, що знаходяться у розпорядженні аналітиків;

– виставкові експонати і проспекти, брошури конкуруючих фінансових посередників;

– звіти власних фінансових аналітиків;

– вивчення асортименту послуг конкуруючих фінансових посередників;

– використання даних, отриманих під час бесід із службовцями конкуруючих організацій (без порушення законів);

– замасковані опитування і «виуджування» інформації у працівників конкуруючих організацій на науково-технічних конгресах (конференціях, симпозіумах);

– бесіди про найом на роботу із працівниками конкуруючих суб'єктів (хоча інтерв'юер зовсім не має наміру брати даної людини до штату своєї організації);

– найм на роботу працівника конкуруючої організації для отримання необхідної інформації;

– співробітництво з інформаційними агентствами з метою одержання інформації;

– використання мережі Internet;

– офіційні зв'язки з органами державного керування всіх рівнів;

– використання бази даних наукових організацій, фондів, бібліотек, архівів;

– одержання відкритої і закритої інформації за допомогою контактів співробітників фінансового посередника з представниками різних державних і комерційних підприємств та інших компетентних осіб.

З метою комплексного забезпечення належного рівня економічної безпеки фінансового посередника у умовах подолання наслідків глобальної фінансово-економічної кризи, необхідно гарантувати повне, вчасне та достовірне інформаційно-аналітичне забезпечення. Таким чином, задачі аналітика у процесі обробки розрізнених даних та перетворення їх на достовірну інформацію зводяться до наступного:

1) оцінки інформації (визначення міри її вірогідності);

2) обробки інформації («очищення» інформації від «шуму» (неупорядкованих, незрозумілих або зайвих відомостей);

3) створення на основі наявної інформації прогнозу розвитку ситуації (на яку дана інформація має або матиме вплив).

Належним чином проаналізована інформація та отриманий аналітиком прогноз направляються до адресата (одразу до керівника або спочатку до начальника служби економічної безпеки, а уже потім до керівника), який:

1) дає оцінку проекту розвитку ситуації;

2) здійснює пошук альтернатив;

3) приймає остаточне рішення щодо напряму використання інформації у процесі діяльності фінансового посередника та вчинення або не вчинення ним на з її врахуванням певних дій.

Належне виконання аналітиками зазначених функцій, зважене прийняття керівництвом установ та організацій управлінських рішень на основі ефективно функціонуючої системи інформаційної безпеки, дозволить забезпечити належний рівень економічної безпеки фінансових посередників.

6.2 Особливості управління системою фінансово-економічної безпеки підприємства

Процес управління системою фінансово-економічної безпеки підприємства забезпечує мінімізацію ризиків, які виникають в процесі його діяльності. Актуальним завданням, яке має вирішувати будь-яке підприємство, є оцінювання ризиків і прогнозування фінансово-економічного стану з огляду виконання властивих йому функцій, впровадження заходів їх захисту від впливу різних внутрішніх і зовнішніх факторів.

Фінансово-економічна безпека досягається здійсненням єдиної, узгодженої, збалансованої, скоординованої системою заходів, адекватних внутрішнім та зовнішнім загрозам. Без створення єдиної системи фінансово-економічної безпеки підприємства неможливо домогтися виходу з кризи, стабілізувати економічну ситуацію, створити ефективні механізми соціального захисту населення.

Система фінансово-економічної безпеки підприємства буде ефективною за умов визначення стратегії і тактики. Стратегія фінансово-економічної безпеки передбачає визначення мети і завдань системи фінансово-економічної безпеки, напрямів їх вирішення, а також форм і способів застосування відповідних сил і засобів, можливість їх перегрупування, створення необхідних резервів для нейтралізації та локалізації можливих загроз.

Тактика фінансово-економічної безпеки – це найбільш гнучка частина системи фінансово-економічної безпеки, яка змінюється залежно від дії внутрішніх і зовнішніх загроз, зміни пріоритетності економічних інтересів тощо. Складність та мінливість економічної та соціальної ситуації вимагає застосування різноманітних тактичних заходів щодо забезпечення фінансово-економічної безпеки підприємства.

Важливо чітко розмежувати стратегічні цілі і тактичні заходи. Стратегія фінансово-економічної безпеки повинна включати:

– характеристику та класифікацію внутрішніх і зовнішніх загроз економічній безпеці;

– визначення і моніторинг факторів, які підривають стійкість фінансового становища підприємства;

– визначення критеріїв і параметрів, які характеризують фінансово-економічні інтереси і відповідають поставленим вимогам;

– формування фінансово-економічної політики та необхідного механізму, що усуває або пом'якшує дію факторів, які підривають стійкість системи фінансово-економічної безпеки;

– основні напрями фінансово-економічної безпеки;

– управління системою фінансово-економічної безпеки, координація діяльності та управління щодо забезпечення фінансово-економічної безпеки на всіх рівнях.

Всі управлінські рішення в галузі забезпечення захисту фінансово-економічних інтересів підприємства, від зовнішніх і внутрішніх загроз, взаємопов'язані і мають прямий або непрямий вплив на результати його діяльності. Захист обумовлений здатністю органів управління підприємства на відповідних рівнях: забезпечити сталий економічний розвиток підприємства; нейтралізувати негативний вплив кризових явищ економіки; сформувати адекватну систему обліку фінансових потоків і зміцнити операційну ефективність системи контролю; забезпечити проведення робіт із захисту конфіденційності інформації, що становить комерційну таємницю тощо.

Головною метою системи фінансово-економічної безпеки підприємства є забезпечення його стійкого і максимально ефективного функціонування, створення високого потенціалу розвитку і зростання в майбутньому.

Система фінансово-економічної безпеки повинна функціонувати в таких режимах:

– повсякденному;
– підвищеної готовності;
– глобального застосування;
– локального застосування.

В системі фінансово-економічної безпеки підприємства особливим є застосування блокової схеми регулювання:

– прогресивне управління витратами підприємства;
– бюджетування;
– управління грошовими коштами;
– діагностика стану підприємства;
– управління оборотними коштами;
– застосування міжнародних стандартів забезпечення безпеки;
– податкове планування тощо.

Основними інструментами забезпечення фінансово-економічної безпеки підприємства в сучасних умовах є фінансовий аналіз та фінансовий менеджмент, включаючи фінансове планування і прогнозування, бюджетування, ризик-менеджмент.

Система фінансово-економічної безпеки підприємства повинна відповідати таким основним вимогам:

– функціонування в межах, визначених законом;

– забезпечення надійного захисту інтересів;

– прогнозування і своєчасне відвернення загроз фінансово-економічній безпеці підприємства;

– ефективне функціонування як у звичайних так і в надзвичайних умовах;

– наявність чіткої структури і функціональне розмежування повноважень керованої та керуючої системи.

Таким чином, розробка методики управління системою фінансово-економічної безпеки підприємства, визначення основних її індикаторів та інструментів забезпечення, створення стратегії фінансово-економічної безпеки і виконання всіх вимог даної стратегії дозволить підприємству запобігти збитку від негативних впливів на його безпеку з різних аспектів фінансово-господарської діяльності, а також забезпечить контроль і балансування доходів і витрат.

До функціональної структури механізму управління фінансовою безпекою можна віднести такі основні функції управління:

– планування, включаючи програмування і прогнозування (розробка оперативних та стратегічних планів, концепцій та програм розвитку, прогнозів);

– організацію і регулювання (вироблення і реалізація управлінських рішень; розробка і використання фінансових інструментів);

– стимулювання (використання економічних та соціально-психологічних методів управління; зростання ефективності праці);

– контроль у складі обліку, аналізу і аудиту (формування контрольно-аналітичної інформації виконання планів, програм; аудит стану фінансової безпеки підприємства).

Управління фінансово-економічною безпекою має здійснюватися за певними правилами і принципами. Аналіз і узагальнення ряду наукових джерел свідчить про те, що виконання завдань і функцій системи фінансово-економічної безпеки здійснюється у разі дотримання ряду основних принципів управління фінансово-економічною безпекою підприємства:

– розроблення системи безпеки на основі й відповідно до чинного законодавства України й нормативних актів із безпеки підприємства; усі прийняті управлінські рішення повинні мати легітимний характер і не суперечити чинному законодавству (принцип законності);

– усі елементи системи управління фінансово-економічною безпекою підприємства мають бути взаємопов’язані та взаємоузгоджені (принцип системності побудови);

– ефективність роботи системи безпеки має бути вищою від її вартості (принцип економічної доцільності);

– витрати на заходи з ліквідації, нейтралізації чи мінімізації загроз фінансово-економічним інтересам підприємства мають бути меншими, ніж можливі збитки від їх реалізації (принцип ефективності управлінських рішень);

– своєчасне попередження та/або ефективне подолання негативного впливу загроз, при цьому забезпечуючи розвиток підприємства (принцип результативності);

– витрати на попередження та/або подолання загроз повинні бути адекватними їх рівню та обсягу (принцип оптимізації витрат);

– всі заходи щодо безпеки повинні проводитися з використанням сучасних досягнень науки й техніки, надавати надійний захист на певних рівнях безпеки (принцип обґрунтованості);

– системність вирішення питань економічної безпеки із залученням усіх суб'єктів та активів підприємства (принцип комплексності);

– забезпечення збалансованості фінансових інтересів підприємства, окремих його підрозділів і персоналу (принцип збалансованості);

– своєчасність розроблення та вживання заходів із нейтралізації загроз фінансовій безпеці і фінансовим інтересам підприємства; всі дії системи безпеки повинні мати попереджувальний характер, а розробка можливих заходів та алгоритмів дій з безпеки повинна проводитися на ранніх стадіях організації системи безпеки на підставі аналізу моделей загроз, дій конкурентів, об'єктів захисту (принцип своєчасності);

– процес управління фінансово-економічною безпекою підприємства має відбуватися безперервно (принцип безперервності);

– постійний системний моніторинг підрозділами економічної безпеки даних про фінансово-економічний стан підприємства та його аналіз з метою недопущення внутрішніх загроз діяльності підприємства; моніторинг зовнішнього середовища підприємства (у зв'язку з його високим динамізмом та невизначеністю) з метою своєчасного виявлення та ідентифікації загроз фінансово-економічним інтересам підприємства (принцип постійного моніторингу);

– реалізація активних дій та заходів захисту фінансово-економічних інтересів підприємства із використанням нестандартних форм і способів захисту (принцип активності);

– координація заходів щодо забезпечення фінансової безпеки на підприємстві; організація взаємодії заходів зі всіма підрозділами підприємства й здійснення єдиного управління процесом безпеки підприємства, організація взаємодії з державними й правоохоронними органами (принцип координації й взаємодії);

– єдиний підхід до виконання своїх функцій учасниками процесу забезпечення безпеки за координаційної ролі та методичного керівництва з боку підрозділу економічної безпеки підприємства; керування безпекою повинен здійснювати перший керівник підприємства (принцип централізації управління);

– система управління фінансово-економічною безпекою підприємства має бути органічно інтегрована у загальну систему менеджменту та загальну

систему управління економічною безпекою підприємства (принцип інтегрованості);

– усі прийняті управлінські рішення не повинні суперечити загальній стратегії фінансово-економічного розвитку підприємства (принцип спрямованості на стратегічні цілі);

– управлінські рішення мають розроблятися з урахуванням об'єктивних економічних законів, на основі глибокого аналізу ситуації із застосуванням наукових методів пізнання (принцип об'єктивності);

– система управління фінансово-економічною безпекою має забезпечувати швидку реакцію на появу реальних та потенційних загроз, своєчасне прийняття відповідних управлінських рішень (принцип оперативності та динамічності);

– кожне управлінське рішення у сфері фінансово-економічною безпеки повинне розроблятися у кількох альтернативних варіантах, враховуючи визначені критерії (принцип варіативності);

– заходи стосовно реагування на загрози фінансово-економічним інтересам підприємства мають розроблятися відповідно до визначених критеріїв (принцип адекватності реагування);

– система управління фінансово-економічною безпекою підприємства, її елементи мусять адаптуватися до зміни чинників зовнішнього та внутрішнього середовища підприємства (принцип адаптивності);

– розроблені чи прийняті управлінські рішення мають швидко коригуватися, якщо цього вимагає зміна зовнішнього чи внутрішнього середовища підприємства (принцип гнучкості управління);

– необхідність і своєчасність удосконалення системи фінансової безпеки підприємства; здатність системи до розвитку і удосконалення (принцип розвитку і удосконалення);

– створення стимулів для ефективного використання ресурсного потенціалу, запровадження інноваційних проектів; має бути розроблена дієва і ефективна система стимулів та відповідальності посадових осіб за стан фінансово-економічної безпеки підприємства (принцип стимулювання та відповідальності).

Реалізація наведеної системи принципів управління фінансово-економічною безпекою підприємства дає змогу забезпечити виконання мети її організації й реалізацію поставлених задач. Суб'єкти управління впливають на об'єкти управлінського впливу за допомогою певних методів управління, які розкривають шляхи протидії реальним та потенційним загрозам, небезпекам та ризикам у конкретних умовах та у визначений термін часу і відображають безпосередній стан захищеності підприємства.

Механізм забезпечення фінансово-економічної безпеки включає такі методи управління, як: інституційно-правові, адміністративні (організаційно-розпорядчі), економічні, організаційно-технологічні, інформаційні, соціально-психологічні.

Забезпечення фінансово-економічної безпеки в рамках інституційно-правових методів передбачає: запровадження моніторингу рівня економічної безпеки та її складових, зокрема фінансової безпеки; прогнозування загроз, ризиків та розробку заходів з їх нейтралізації; коригування планових показників діяльності у контексті забезпечення економічної безпеки; розробку системи правил та режимів безпеки; створення інструкцій про матеріальну відповідальність та захист комерційної таємниці; моніторинг законодавства та захист підприємства від дій і рішень органів державного управління; управління інституційними характеристиками безпеки в межах юридичних відносин із контрагентами; реєстрацію документів, прав власності.

За допомогою адміністративних (організаційно-розпорядчих) методів управління відбувається: формування організаційної структури управління фінансово-економічною безпекою; визначення повноважень та відповідальності посадових осіб, розпорядку роботи, порядку дій у тій чи іншій ситуації; регламентування інших дій суб'єктів управління фінансово-економічною безпекою; введення режимів входу/виходу персоналу та відвідувачів; створення перешкод для доступу до охоронного майна.

Забезпечення фінансово-економічної безпеки економічними методами передбачає: реалізацію заходів, спрямованих на підвищення ефективності використання господарських ресурсів; оцінку рівня сучасності та продуктивності матеріально-технічної бази, пошук резервів її покращення; підвищення рентабельності активів та конкурентоспроможності підприємства; фінансування заходів із прогнозування розвитку ринкової кон'юнктури, інституціонального регламентування фінансово-господарської діяльності та ресурсного забезпечення.

Організаційно-технологічні методи спрямовані на підвищення ефективності управління безпекою шляхом впровадження на підприємстві міжнародних систем управління якістю.

Інформаційні методи передбачають створення механізму оперативного реагування на загрози інформаційній безпеці та поширення негативної інформації про підприємство. Заходами щодо забезпечення фінансово-економічної безпеки даною групою методів виступають: аналіз, облік комерційної інформації; створення надійної системи захисту інформації та каналів її проходження; використання сучасних технологій захисту інформації (систем кодування і шифрування).

Застосування соціально-психологічних методів передбачає: реалізацію заходів матеріального стимулювання; створення ефективної системи морального заохочення працівників; підбір кадрів з урахуванням психологічних характеристик працівників; діагностику психоемоційного стану працівників; підтримку ініціативи; забезпечення перспективного соціального й професійного росту; інформування про результати праці; укладання договорів, взаємних зобов'язань, об'єднання інтересів працівників; бесіди, пропаганду та агітацію, призначені для поширення і роз'яснення політики керівництва у сфері фінансової безпеки; розробку правил поведінки; створення атмосфери

корпоративного духу; формування сприятливого морально-психологічного клімату в колективі; формування неформальних комунікацій.

В управлінні фінансово-економічною безпекою підприємства необхідне застосовування всіх зазначених груп методів управлінського впливу, які реалізуються комплексно, безперервно та оперативно.

Управління фінансовою безпекою неможливо без відповідної організаційної структури.

Головними чинниками, які визначають організаційну структуру управління фінансово-економічною безпекою на підприємстві, виступають: вид економічної діяльності підприємства; його організаційно-правова форма; характеристики ринку, на якому діє підприємство (рівень та методи конкуренції, особливості попиту тощо) та його ринкова позиція (частка ринку, рівень конкурентоспроможності та ін.); обсяг фінансово-економічної діяльності підприємства; головні види фінансово-економічної діяльності підприємства; досягнутий рівень фінансово-економічної безпеки; наявність та кількість регіональних відділень; кількість та професійно-кваліфікаційний рівень працівників; можливість фінансового забезпечення функціонування системи управління фінансово-економічною безпекою підприємства; стиль керівництва (менеджменту); погляди власників та керівників підприємства на необхідність та принципи побудови системи управління фінансово-економічною безпекою тощо.

Призначення інформаційного забезпечення у механізмі управління фінансовою безпекою підприємства полягає у своєчасному формуванні та видачі достовірної та повної інформації для прийняття управлінських рішень. Інформація в системі забезпечення економічної безпеки підприємства є предметом аналізу і одночасно продуктом кінцевої праці. Вхідні дані аналізуються, переробляються і передаються далі у вигляді службової інформації, рекомендацій, звітів, рішень. Обмін інформацією здійснюється в тому вигляді і тими способами, які передбачені правилами внутрішнього документообігу на підприємстві. Обмін інформацією між учасниками системи забезпечення економічної безпеки здійснюється за допомогою інформаційної системи. Для формування інформаційного забезпечення і його ефективного застосування на підприємстві в процесі організації економічної безпеки, необхідно: визначення мети, задач, функцій всієї системи управління підприємством; виявлення руху інформації на підприємстві та формування схем інформаційних потоків; удосконалення системи документообігу; створення інформаційно-логічних моделей, які відображають взаємозв’язок інформації; створення масивів інформації у вигляді інформаційних баз даних тощо.

6.3 Формування системи обліково-аналітичного забезпечення фінансово-економічної безпеки підприємства

Ризиковість ведення бізнесу визначають такі фактори, як: сезонність виробництва, залежність від погодних та кліматичних умов, тривалий період

обороту капіталу, велика складність зміни асортименту продукції та технології, ряд інших причин. Дане твердження справедливе для економіки всіх країн, але особливо великих ризиків зазнає виробництво країн, економіки яких розвиваються або перебувають в процесі трансформації. Реформи та становлення ринкових взаємовідносин, зміна форм власності та форм господарювання значно збільшують ступінь невизначеності соціально-економічних процесів в бізнес-середовищі і, відповідно, підсилюють вплив ризиків на бізнес.

В системі ризиків особлива увага відводиться – фінансовим. Фінансовий ризик пов’язаний з отриманням, розміщенням і використанням фінансових ресурсів. Основні причини виникнення фінансових ризиків, автор виділяє наступні: несприятливі зміни процентних ставок, непередбачене скорочення терміну повернення привернутих засобів, недолік кредитних ресурсів, зниження рентабельності або збитковість виробництва, висока питома вага позикового капіталу в структурі пасивів підприємства, відсутність резервів високоліквідних активів. Тож фінансові ризики, пов'язані з діяльністю підприємств за своїми негативними наслідками відносяться до категорії найбільш небезпечних. Реалізація багатьох видів фінансових ризиків формує безпосередню загрозу втрати підприємством значної частини власного капіталу, зниження рентабельності, фінансової стійкості, ліквідності, що призводить до банкрутства і ліквідації суб’єкта господарювання.

В такій ситуації підприємства можуть ефективно господарювати в сучасному бізнес-середовищі лише за умови побудови механізму фінансової безпеки. Своєчасна оцінка фінансової безпеки підприємств є передумовою запобігання фінансових загроз і негативних фінансових явищ у виробничій діяльності, захисту їх від фінансових втрат, а в подальшому стабілізації діяльності сільськогосподарських формувань і розвитку в умовах конкурентного економічного стану.

Дієвість фінансової безпеки підприємств потребує належного інформаційного забезпечення, під яким розуміють сукупність документів і даних, які в них знаходяться, а також методів і засобів їх одержання, організації зберігання й обробки.

В сучасних умовах інформація виступає рушієм будь-якого бізнесу. Вона допомагає правильно оцінити умови бізнес середовища, усвідомити та сформувати цілі та завдання майбутньої діяльності та на цій основі прийняти ефективні управлінські рішення.

Інформація є визначальним чинником, що характеризує рівень безпеки бізнесу. Висока поінформованість керівників та менеджерів про бізнес-процеси та загрози дозволяє мінімізувати ризики та забезпечити конкурентні переваги.

В інформаційній системі підприємства левова частка припадає на обліково-аналітичну інформацію.

Облік є базою для аналізу, а результати аналізу, у свою чергу, є підставою для проведення синтезу та надання відомостей потенційному користувачеві цієї інформації.

В економічній літературі зустрічаються різні підходи до трактування терміну «обліково-аналітичне забезпечення».

Обліково-аналітичним забезпеченням – процес підготовки обліково-аналітичної інформації, забезпечення її кількості та якості. Термін «забезпечення», означає виконання, гарантування здійснення процесу постачання обліково-аналітичної інформації системі управління.

Обліково-аналітичне забезпечення являє собою сукупність процесу збору, підготовки, реєстрації та зведення облікової інформації підприємств залежно від законодавчо встановленої системи ведення обліку, і проведеного на основі цієї інформації глибокого аналізу із застосуванням певних методів і прийомів.

З представлених визначень бачимо, що науковці в основному трактують термін «обліково-аналітичне забезпечення» як процес збору інформації за рахунок обліку та аналізу для цілей управління.

Виходячи із цього під обліково-аналітичним забезпеченням управління фінансовою безпекою підприємств, можна розуміти процес збору, підготовки, реєстрації та обробки обліково-аналітичної інформації та прийняття на її основі управлінських рішень направлених на забезпечення захисту фінансових інтересів підприємств на всіх рівнях його фінансових відносин від впливу внутрішніх і зовнішніх загроз.

Основою обліково-аналітичного забезпечення є інформація, тобто сукупність відомостей про внутрішнє і зовнішнє середовище підприємства, яку використовують для оцінки й аналізу економічних явищ та процесів для розроблення і прийняття управлінських рішень. Слід зауважити, що управління економічною безпекою підприємства — це неперервний процес отримання інформації про рівень безпеки та ймовірність виникнення та розвитку викликів, загроз і ризиків з подальшим напрацюванням адекватних до ситуації управлінських рішень. Відповідно до цього, обліково-аналітична інформація має відповідати таким вимогам:

– чітко та достовірно відображати в зовнішній та внутрішній звітності всі господарські операції, що здійснюються на підприємстві;

– подавати суб’єктам безпеки інформацію про поточний рівень економічної безпеки шляхом розрахунку найважливіших якісних та кількісних показників;

– виявляти, ідентифікувати та відстежувати розвиток внутрішніх та зовнішніх викликів, ризиків та загроз;

– протидіяти промисловому шпигунству та витоку конфіденційної інформації;

– формувати інформаційну базу для прийняття рішень у процесі управління економічною безпекою підприємства.

Обліково-аналітична інформація є результатом функціонування відповідної системи забезпечення.

Обліково-аналітична система – це інтегрована система прийомів обліково-аналітичного забезпечення менеджменту шляхом здійснення специфічних внутрішньо системних та загальносистемних функцій.

Система обліково-аналітичного забезпечення відіграє важливу роль у функціонуванні системи управління підприємством, забезпечуючи взаємодію різних структурних підрозділів та реагуючи на зміни внутрішнього й зовнішнього середовищ.

Підсумовуючи можна стверджувати, що обліково-аналітична система – це система, що ґрунтується на даних оперативного, статистичного, фінансового й управлінського обліку, включаючи оперативні дані, і використовуючи для економічного аналізу статистичну, виробничу, довідкову та інші види інформації шляхом застосування аналітичних і економіко-математичних методів дослідження, що уможливлює формування інформаційної бази для прийняття адекватних до ситуації рішень, зокрема в межах системи економічної безпеки підприємства.

Основними завданнями для обліково-аналітичної системи підприємства повинні бути:

– аналіз діяльності підприємства за вказаними напрямами;

– облік господарських операцій за цільовими напрямами на базі бухгалтерського обліку з додаванням нефінансових показників;

– контроль за використанням матеріальних та нематеріальних ресурсів, за правильним відображенням усіх господарських операцій на етапах планування, обліку та за достовірністю аналітичних даних;

– планування діяльності підприємства, зокрема господарських операцій; видів діяльності: операційної, інвестиційної, фінансової, податкової; центрів відповідальності та підприємства загалом;

– формування аналітичних бюджетів як джерел акумулювання планової, облікової та аналітичної інформації.

Ключове завдання системи обліково-аналітичного забезпечення як складової системи економічної безпеки підприємства полягає в об’єднанні облікових та аналітичних операцій в єдиний процес, виконання оперативного мікроаналізу, забезпеченні безперервності цього процесу і використанні його результатів для формування інформаційної бази для прийняття управлінських рішень.

Зміст обліково-аналітичного забезпечення управління економічною безпекою підприємства визначається низкою факторів, серед яких: галузеві особливості діяльності підприємства, організаційно-правова форма функціонування, обсяг і ступінь диверсифікації фінансово-господарської діяльності, інші об'єктивні та суб'єктивні фактори.

Звідси можна сформулювати основні функції обліково-аналітичного забезпечення системи управління фінансовою безпекою підприємств:

1) інформаційна – забезпечення системи управління інформацією про фінансово-господарську діяльність підприємства;

2) облікова – достовірне та повне відображення фактів господарської діяльності підприємств;

3) аналітична – здійснення на підставі даних обліку та звітності оцінки та рівня фінансової безпеки підприємств.

Процес функціонування системи обліково-аналітичного забезпечення можна схематично зобразити наступним чином (рис. 6.1).

На нашу думку, механізм обліково-аналітичного забезпечення має передбачати збирання інформації, способи її узагальнення та аналізу, а також технології надання безпосереднім користувачам для оцінки рівня та стану економічної безпеки власного підприємства чи його партнерів та/або конкурентів, діяльність яких може вплинути на стан безпеки підприємства.

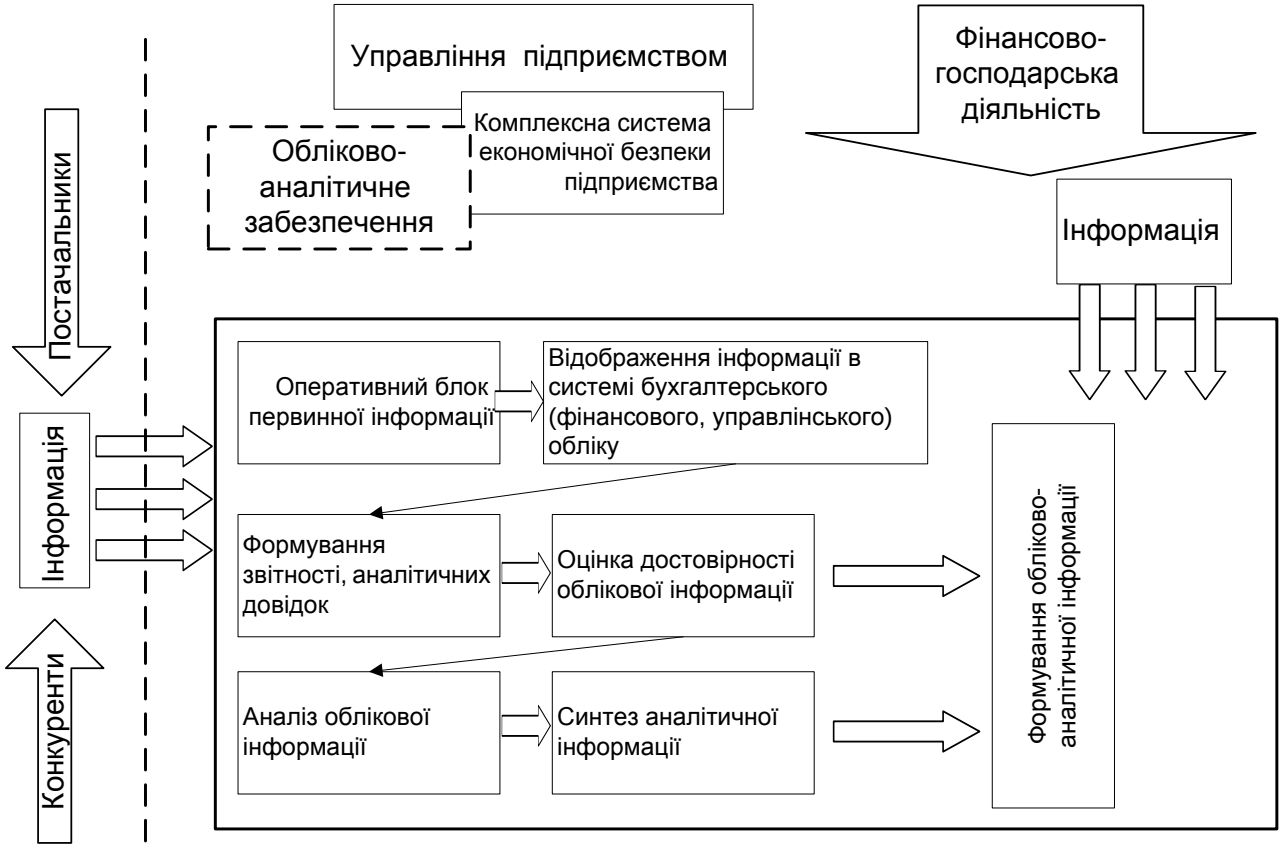

Рис. 6.1. Процес функціонування системи обліково-аналітичного забезпечення

Отже, на основі вище поданого можна сформувати основні напрями здійснення обліково-аналітичного забезпечення в системі економічної безпеки підприємства:

– інформаційне забезпечення прийняття рішень суб’єктами безпеки;

– моніторинг рівня економічної безпеки підприємства;

– виявлення та ідентифікація появи та розвитку ключових внутрішніх і зовнішніх загроз та ризиків;

– подання достовірної інформації про наявні ресурси;

– надання інформації про рівень агресивності зовнішнього середовища;

– узгодження економічних інтересів підприємства.

Ефективне функціонування системи економічної безпеки підприємства залежить передусім від можливості отримати та використати за прямим призначенням якісну інформацію про зміну зовнішнього і внутрішнього середовищ певного суб'єкта господарювання. Задоволення інформаційних потреб користувачів – суб'єктів економічної безпеки – є головним завданням обліково-аналітичної системи.

Загалом зміст обліково-аналітичного забезпечення фінансової безпеки, визначається низкою факторів, серед яких галузеві особливості діяльності підприємств, організаційно-правова форма функціонування, обсяг і ступінь диверсифікації фінансово-господарської діяльності, інші об'єктивні та суб'єктивні фактори.

Формування ефективної системи обліково-аналітичного забезпечення фінансової безпеки підприємств передбачає виконання комплексу завдань. До них необхідно віднести:

–достовірне та повне відображення в обліку та звітності даних, необхідних для оцінки стану та рівня фінансової безпеки підприємств;

–розробка критеріїв та порядку оцінки якості інформації, яка створюється у системі обліку та аналізу для ідентифікації та оцінки ризиків та загроз;

–визначення індикаторів фінансової безпеки підприємств та розробка системи моніторингу фінансової безпеки;

–діагностика фінансового стану підприємств з метою упередження фінансових ризиків, ідентифікації небезпек і загроз;

–прийняття управлінських рішень щодо доцільності діяльності з урахуванням виявлених загроз та небезпек;

–розробка заходів, направлених на забезпечення фінансової безпеки підприємства, як в короткостроковому, так і в довгостроковому періоді та контроль за їх виконанням.

Структурна схема системи обліково-аналітичного забезпечення схематично зобразимо на рис. 6.2.

Сучасна система обліково-аналітичного забезпечення фінансової безпеки підприємств потребує нового сутнісного наповнення як комплексу взаємодіючих та взаємопов'язаних методів, методик, процедур і моделей, призначених для обґрунтування прийняття управлінських рішень в сфері забезпечення фінансової безпеки підприємства. Вона має включати в себе усі без винятку інструменти обліку та аналізу з метою отримання синергетичного ефекту від їх системного застосування при: забезпеченні стабільного та стійкого фінансового стану підприємства; збалансуванні фінансово-матеріальних потоків і розрахункових відносин; нейтралізації впливу внутрішніх та зовнішніх загроз на фінансово-господарський стан підприємства; зниженні рівня інформаційного та фінансового ризику тощо.

Рис. 6.2 Структурна схема системи обліково-аналітичного забезпечення фінансової безпеки підприємства

Проведені дослідження системи обліково-аналітичного забезпечення фінансової безпеки підприємств дають можливість зробити такі узагальнення:

– під обліково-аналітичним забезпеченням управління фінансовою безпекою підприємств слід розуміти процес збору, підготовки, реєстрації та обробки обліково-аналітичної інформації та прийняття на її основі управлінських рішень направлених на забезпечення захисту фінансових інтересів підприємств на всіх рівнях його фінансових відносин від впливу внутрішніх і зовнішніх загроз;

– при формуванні системи обліково-аналітичного забезпечення фінансової безпеки підприємств необхідно враховувати фактори, які визначають ризиковість певного виду бізнесу: сезонність виробництва, залежність від погодних та кліматичних умов, тривалий період обороту капіталу, велика складність зміни асортименту продукції та технології, ряд інших причин;

– сучасна система обліково-аналітичного забезпечення фінансової безпеки підприємств потребує нового сутнісного наповнення. Вона має включати всі інструменти обліку та аналізу з метою отримання синергетичного ефекту від їх системного застосування при: забезпеченні стабільного та стійкого фінансового стану підприємства; збалансуванні фінансово-матеріальних потоків

і розрахункових відносин; нейтралізації впливу внутрішніх та зовнішніх загроз на фінансово-господарський стан підприємства; зниженні рівня фінансового ризику.

Контрольні питання:

1. Головна мета інформаційного забезпечення фінансово-економічної безпеки.
2. Основні цілі фінансово-економічної безпеки на підприємстві.
3. Завдання фінансово-економічної безпеки на підприємстві.
4. Основна мета аналітичного забезпечення фінансово-економічної безпеки.
5. Інформаційна безпека: сутність та особливості.
6. Фактори впливу на інформаційно-аналітичне забезпечення фінансово-економічної безпеки на підприємстві.
7. Основні джерела інформації.
8. Шляхи отримання інформації.
9. Основні задачі аналітика в процесі отримання інформації.
10. Основні задачі керівника при інформаційно-аналітичній роботі.
11. Особливості управління системою фінансово-економічної безпеки на підприємстві.
12. Складові стратегії фінансово-економічної безпеки на підприємстві.
13. Режими системи фінансово-економічної безпеки на підприємстві.
14. Вимоги до системи фінансово-економічної безпеки на підприємстві.
15. Принципи здійснення управління фінансово-економічної безпеки.
16. Методи управління механізму забезпечення фінансово-економічної безпеки.
17. Формування системи обліково-аналітичного забезпечення фінансово-економічної безпеки.
18. Вимоги до системи обліково-аналітичного забезпечення фінансово-економічної безпеки.
19. Основні завдання системи обліково-аналітичного забезпечення фінансово-економічної безпеки.
20. Функції системи обліково-аналітичного забезпечення фінансово-економічної безпеки.

Тема 7. *Визначення небезпек, загроз та ризиків у фінансово-економічній сфері*

План:

7.1 Зовнішні та внутрішні ризики та загрози у сфері фінансово-економічної безпеки підприємства.

7.2 Дослідження ризиків та загроз економічній безпеці у всіх сферах діяльності підприємства.

7.3 Методологія діагностування ризиків, загроз та небезпек, їх оцінка та мінімізація.

7.4 Проведення контролю та оцінка рівня фінансово-економічної безпеки на підприємстві.

7.1 Зовнішні та внутрішні ризики та загрози у сфері фінансово-економічної безпеки підприємства

Рівень фінансово-економічної безпеки характеризує здатність підприємства протистояти її загрозам або усувати збитки від негативних впливів на різноманітні аспекти безпеки.

Під загрозою фінансово-економічній безпеці розуміють потенційні або реальні дії фізичних чи юридичних осіб, що порушують стан захищеності суб'єкта підприємницької діяльності та здатні призвести до припинення його діяльності або до фінансових й інших втрат.

Загрози відображають зовнішні та внутрішні умови, в яких здійснює свою діяльність підприємство, а також взаємозв'язки підприємства з навколишнім середовищем. Загроза фінансовій безпеці підприємства кількісно може визначатися як величина збитку або інший інтегральний показник, що характеризує ступінь зниження економічного потенціалу підприємства.

Загрози фінансовій безпеці підприємницької діяльності відрізняються різноманітністю. Можна навести таку узагальнену класифікацію загроз фінансовій безпеці підприємства.

При визначенні загроз необхідно керуватися рядом параметрів:

– реальністю загрози;
– суттю протиріч, що породили загрозу;
– гостроту цих протиріч;
– терміновість їх вирішення;
– визначенням сил і засобів, якими може послужитися і скористатися опонент;
– розробкою і виявленням ознак можливої загрози.

Крім того, необхідно розробити систему ознак та етапів підготовки і здійснення загрози, вироблення прогнозів і рекомендацій по локалізації загроз.

Варто зазначити, що у наукових публікаціях часто зустрічаються доволі схожі підходи до поділу ризиків функціонування підприємства чи їх сукупності. Відповідно, загальна (традиційна) класифікація загроз економічній

безпеці підприємництва може здійснюватись за такими ознаками, як: спосіб впливу на об'єкт; масштаб збитків від дії загрози; мета загрози; сфера діяльності об'єкта тощо.

Насамперед загрози економічній безпеці підприємництва за джерелом виникнення небезпеки варто поділяти на внутрішні та зовнішні.

До зовнішніх загроз можна віднести наступні:

– зріст промислового шпіонажу із використанням агентурного та технічного проникнення в комерційні, технологічні та виробничі таємниці підприємства;

– безготівкова форма розрахунків із використанням комп'ютерних систем;

– несанкціоноване проникнення в банки даних;

– відсутність єдиної діючої стратегії забезпечення безпеки бізнесу і механізму її реалізації;

– недобросовісна конкуренція, яка часто носить кримінальні форми;

– кризові явища в економіці;

– непередбачувані зміни кон'юнктури ринку;

– соціальна напруженість;

– надзвичайні ситуації;

– адміністративні переслідування, направлені на ринок;

– несприятлива для приватного бізнесу економічна політика держави;

– маніпулювання обліковою ставкою, валютним курсом, митними платежами та податками;

– необґрунтовані зміни у системі державного регулювання підприємницької та господарської діяльності;

– загрози, що походять від неузгоджених нормативних актів, що видаються законодавчими та виконавчими органами держави, а також різними міністерствами і відомствами, які іноді протирічать законам і один одному, однак все одно підлягають виконанню.

Як бачимо із наведеного, далеко не повного, списку зовнішніх загроз, більшість із них пов'язана із діяльністю держави, зокрема державним управлінням. Саме державне управління може розцінюватись в одному випадку як загроза економічній безпеці підприємства, а з іншого – як елемент мінімізації комплексу загроз, які створюють небезпеку для підприємства. Тобто, державне регулювання, в залежності від його спрямування і цілей, можна розглядати і як позитивне і як негативне явище. Основоположною метою при цьому можна визначити необхідність зменшення його негативного пливу і збільшення позитивного впливу на стан економічної безпеки підприємства.

Як вважає Т.Г. Васильців, передумовою належного аналізу внутрішніх загроз економічній безпеці підприємництва є комплексна їх оцінка. Зокрема, розгляд її за системним підходом з урахуванням сукупності взаємопов'язаних елементів системи (в якій зміна одного зачіпає інтереси інших та/чи усіх

елементів системи) та частин; апарату управління та загальних механізмів прийняття рішень; спільної мети та завдань; підсистем.

Основне, що системний підхід має містити визначення переліку суб'єктів, елементів та їх інтересів, функцій, засобів забезпечення таких інтересів та форм їх фінансування.

Згідно із системним підходом до *внутрішніх загроз економічній безпеці підприємства* доцільно внести:

– настання небажаних змін властивостей, параметрів чи якостей на рівні особи чи підприємства;

– суттєве зниження рівня ефективності фінансово-господарської діяльності та використання критичної маси ресурсного забезпечення підприємства;

– різке погіршення рівня конкурентоспроможності підприємства;

– формування нераціональної та неефективної галузевої структури;

– спад виробництва підприємства тощо.

Враховуючи те, що усі названі загрози об'єктивно є серйозними, дані питання повинні бути постійно в полі зору керівництва підприємства. Як правило, це досягається шляхом підбору кваліфікованих кадрів. Слід враховувати, що жоден юрист чи бухгалтер не в змозі володіти усією багатоманітністю нормативних актів та інструкцій, а також особливостями їх застосування на практиці. Тому доцільним видається для оформлення важливих заходів застосовувати працю сторонніх вузьких спеціалістів, які добре розуміються на тонкощах окремих питань. Як правило, в кінцевому результаті такий хід подій виявляється дешевшим для підприємства.

Економічні загрози можна класифікувати також за сферами, в яких можуть виникати загрози економічній безпеці підприємництва, зокрема: виробничі, галузеві, політичні, економічні, фінансові, інноваційні, юридичні ризики тощо.

Так, до *категорії виробничих* можна віднести ризики, пов'язані з: ускладненням доступу підприємств до господарських ресурсів, засобів праці та технології; критичним зношенням або моральним старінням матеріально-технічної бази; втратою виробничих зв'язків; впровадженням конкурентами аналогічних техніки та технології виробництва товарів чи надання послуг; невиваженістю формування техніко-технологічної політики.

Політичні ризики певною мірою піддаються впливу з боку органів державного управління, проте часто завдають суттєвих збитків окремим суб'єктам господарської діяльності чи підприємництву загалом. Більшою мірою вони пов'язані з надмірною політизацією дій представників органів державної влади та управління, відволіканням їх від виконання своїх функцій, що призводить до зволікання у вирішенні багатьох питань (в тому числі, щодо управління економічною безпекою бізнесу), відтермінуванням прийняття необхідних рішень, спрямованих на розвиток повноцінної інституціональної бази розвитку підприємництва та економіки загалом, «затягуванням» процедур проходження дозвільних та погоджувальних рішень.

Економічні та фінансові ризики, в основному, зумовлені несприятливою кон'юнктурою ринку, що призводить до відхилення фінансово-економічних результатів функціонування підприємств від запланованих; невірним фінансовим плануванням та управлінням активами; невиправданою маркетинговою політикою; недооцінкою фінансових ризиків; форс-мажорними обставинами.

До правових ризиків економічної безпеки підприємництва доцільно віднести недоліки у законодавстві та системі правозастосування, помилки працівників юридичної служби підприємств; недоліки у плануванні юридичного забезпечення їх діяльності; неефективне відстоювання інтересів підприємств у судових та інших інстанціях.

Серед дій, які можна розцінювати як ризики економічній безпеці підприємств, джерелом походження яких є кримінальні структури та окремі злочинці слід назвати:

– економічне проникнення у комерційні структури і підпорядкування їх своєму контролю;

– вимагання коштів, цінних паперів та інших цінностей у підприємств;

– економічний підрив банків і підприємств;

– пошкодження, крадіжки, знищення будівель, засобів виробництва, товарів, сировини, транспортних засобів тощо на замовлення конкурентів або як помста за непідкорення вимогам злочинних угруповань;

– спроби влаштування на роботу на підприємство представників кримінального угруповання;

– пропозиції про надання «покровительства» за відсотки від прибутку;

– скуповування акцій підприємства у низькооплачуваних співробітників;

– компрометування репутації підприємства і його товарів;

– підрив технічної бази підприємства тощо.

Загрози економічній безпеці підприємництва можна розрізняти не тільки за своїм змістом і виникненням, але і за частотою дії. За вказаною класифікацією загрози можна поділяти на:

– одноразові, які можуть виникати одноразово, проте діяти протягом тривалого періоду (або постійно) і чинити негативний вплив на життєво важливі характеристики підприємницького середовища (суттєва зміна законодавства країни, посилення конкуренції між виробниками однорідної продукції і т.ін.);

– багаторазові, які впливають на діяльність підприємства чи їх сукупності або стохастично, або з визначеним періодом виникнення (сезонні коливання попиту на продукцію, загрози стихійних лих, тимчасовий розрив відносин з постачальником або підрядником, нестабільність роботи дилерської мережі й т.ін.).

Розглянемо більш детально характеристики різних видів загроз:

1. За джерелом виникнення всі загрози можна поділити на:

– зовнішні та внутрішні.

Серед *зовнішніх загроз* виділяють розкрадання матеріальних засобів і цінностей особами, що не працюють у цій фірмі, промислове шпигунство, незаконні дії конкурентів, здирство з боку кримінальних структур. До зовнішніх загроз фінансовій безпеці підприємства відносять також спекулятивні операції з цінними паперами підприємства, цінову та інші форми конкуренції, агресивну купівлю акцій підприємства зовнішнім інвестором, лобіювання конкурентами негативних рішень органів влади. Вплив зовнішніх загроз і сили, яку можуть залучатися до їх відображення наведені в таблиці 7.1.

Таблиця 7.1

Зміст та джерела зовнішніх загроз підприємства

Джерела загроз	*Зміст і цілі загрози*	*Відповідальний*
Представники органів державної влади	Проведення перевірок або оперативних заходів за замовленням конкурента. Проведення перевірок або оперативних заходів в ініціативному порядку з метою вимагання хабарів.	Юридична служба Служба безпеки
Кримінальні структури	Виконання «замовлення» по фізичному тиску на підприємство, його партнерів, постачальників і споживачів. Організація нападів на підприємство і його власність в дорозі з метою заволодіння продукцією, фінансами, сировиною.	Юридична служба Служба безпеки Правоохоронні органи
Постачальник	Зміна цінової політики на постачання ресурсів, сировини, комплектуючих. Зміна умов постачання ресурсів, сировини, комплектуючих.	Юридична служба Фінансовий директор Головний інженер Служба безпеки
Споживачі	Відмова від закупівель продукції. Висування вимог щодо зниження закупівельних цін. Вимоги змінити умови поставки на менш вигідні для постачальника.	Служба реалізації продукції Фінансовий директор Головний бухгалтер Юридична служба
Конкуренти	Погрози та шантаж проти керівників. Шпигунство з метою активної протидії нормальної роботи. Вплив на керівників та менеджерів підприємства. Нанесення збитку основним фондам.	Служба безпеки Головний інженер Головний технолог Юридична служба Служба маркетингу
Фінансово-кредитні установи	Несподівана відмова у кредиті. Затримка у проведенні платежів.	Фінансовий директор Головний бухгалтер Юридична служба

Серед *внутрішніх загроз* можна виділити такі, як розголошування власними співробітниками конфіденційної інформації, низька кваліфікація фахівців, неефективна робота служби фінансової або економічної безпеки й осіб, що відповідають за перевірки, неефективне фінансове планування та

управління активами, неефективне управління ринком акцій підприємства, помилки у виборі дивідендної політики (табл. 7.2).

Таблиця 7.2

Зміст і джерела внутрішніх загроз підприємства

Джерела загроз	*Зміст і цілі загрози*	*Відповідальний*
Керівники та менеджери	Шахрайство з метою заволодіння активами компанії. Фальсифікація звітності з метою привласнення грошових коштів. Розкрадання майна в особливо великих розмірах шляхом закупівлі сировини за завищеними цінами, надання пільг партнерам і т.п. Надання або продаж конкурентам інформації, що є комерційною таємницею підприємства. Її використання конкурентами здатне завдати значної, а то і катастрофічний збиток.	Служба безпеки Служба персоналу
Співробітники	Крадіжка продукції, сировини, ресурсів, комплектуючих . Крадіжка фінансових коштів та інформаційних ресурсів. Нецільове та несанкціоноване використання техніки, обладнання, транспорту, інформаційно-обчислювальних засобів та ін. Продаж відомостей, що становлять комерційну таємницю підприємств .	Служба безпеки Служба персоналу Служба внутрішнього аудиту
Працівники	Крадіжка готової продукції, сировини, комплектуючих. Крадіжка фінансових коштів. Нецільове використання транспортних засобів і спеціальної техніки та обладнання. Надання допомоги стороннім у скоєнні протиправних дій на підприємстві з метою нанесення збитку Навмисний виведення з ладу техніки, обладнання, інформаційних ресурсів, псування сировини і пр. за винагороду за замовленням третіх осіб.	Служба безпеки Служба персоналу Керівники структурних підрозділів

2. Залежно від джерела виникнення загрози поділяють на:

– об’єктивні та суб’єктивні.

Об’єктивні загрози фінансовій безпеці підприємства спричинені чинниками та явищами навколишнього середовища і виникають незалежно від прийнятих управлінських рішень. Серед цих загроз варто відзначити стан

світової фінансової кон'юнктури, суспільно-політичні процеси в країні, наукові відкриття, форс-мажорні обставини тощо.

Суб'єктивні загрози спричинені свідомими або несвідомими

3. Загрози поділяються за об'єктом посягань.

Об'єктами посягань виступають насамперед ресурси: трудові (персонал), матеріальні, фінансові, інформаційні. Загрози трудовим ресурсам здатні проявлятися у негативних впливах на фізичний або психологічний стан працівників з метою отримання конфіденційної інформації про підприємство. Результатом реалізації загроз матеріальним ресурсам може бути втрата або псування виробничих фондів підприємства, пошкодження будівель, приміщень, систем зв'язку, зумовлена діями чи бездіяльністю певних суб'єктів.

Ненадійність постачальників та партнерів, фінансово-кредитних установ як результат реалізації загроз фінансовим ресурсам здатна спричинити втрату фінансових ресурсів, зменшення власного капіталу і зниження ринкової вартості підприємства, зменшення фінансової стійкості та ліквідності підприємства. Загрози інформаційним ресурсам полягають у несанкціонованому доступі й розголошуванні науково-технічних розробок, ноу-хау, винаходів, конфіденційної інформації підприємства тощо.

4. За можливістю здійснення загрози фінансовій безпеці поділяються на:

– реальні та потенційні.

Реальні загрози існують об'єктивно в досліджуваний період часу або з достатньо великою ймовірністю здатні виникнути в наступні періоди, тобто їх реалізація є неминучою.

Потенційні загрози можуть настати під час реалізації певних суб'єктивних чи об'єктивних умов.

5. За тривалістю дії загрози поділяють на:

– тимчасові, які діють протягом обмеженого періоду часу,

– постійні, які діють протягом усього періоду існування системи фінансової безпеки підприємства й фактично непереборні.

6. За частотою дії загрози фінансовій безпеці поділяються на:

– одноразові, виникнення яких має одноразовий характер,

– багаторазові, які проявляються час від часу або з певним інтервалом під впливом певних чинників внутрішнього й зовнішнього середовищ.

7. За суб'єктами загроз поділяються на:

– загрози з боку кримінальних структур;
– загрози з боку конкурентів;
– загрози з боку контрагентів;
– загрози з боку власних працівників;
– загрози з боку держави; форс-мажорні загрози.

8. За формою збитку виділяють:

– загрози, реалізація яких завдає прямого збитку,
– загрози, реалізація яких призведе до упущеної вигоди.

Враховуючи різноманітний прояв загроз фінансовій безпеці, одну і ту ж загрозу можна одночасно відносити до різних груп класифікації.

Для досягнення максимального ступеня захисту від цих загроз необхідна певна діяльність, яка повинна забезпечити фінансову безпеку фірми. Розгляд загроз дає змогу підготувати основу для сукупного аналізування ефективності заходів, що застосовуються для забезпечення фінансової безпеки підприємства.

Одним із основних засобів забезпечення ефективного функціонування системи фінансової безпеки підприємства є узгоджене застосування методів оцінювання збитків як бази та інструменту контролю, а також орієнтира під час планування та здійснення фінансово-господарської діяльності підприємства.

З метою управління ризиками суб'єкти управління системою економічної безпеки наділяються рядом функцій. *Так до пріоритетних функцій органів державного управління необхідно віднести:*

– формування нормативно-правової бази, сприятливої для підприємництва;

– здійснення систематичних заходів соціально-психологічного та інформаційно-роз'яснювального характеру серед підприємців та населення;

– формування надійної системи судового та оперативного фізичного захисту громадян і підприємців;

– провадження ефективної податкової, фінансово-кредитної, інноваційно-інвестиційної та інших складників державної політики, які відповідають нормам досконалої регуляторної політики;

– ведення моніторингу рівня безпеки підприємництва;

– регулювання внутрішнього ринку, захист вітчизняних підприємств та забезпечення їх конкурентоспроможності.

Пріоритетними функціями суб'єктів підприємницької діяльності в межах системи економічної безпеки підприємництва мають бути: формування надійних механізмів забезпечення економічної безпеки підприємства на мікрорівні управління, а також забезпечення економічної ефективності діяльності, використання ресурсного забезпечення та суспільної праці.

Основними причинами появи економічних загроз і небезпек для підприємства є, передусім, конфлікт інтересів суб'єктів підприємницького середовища (а також засобів їх досягнення) і дії чинників зовнішнього та внутрішнього середовища його функціонування. Як наслідок, неузгодженість інтересів може являти собою загрозу його розвитку.

Виявлення і вжиття заходів, спрямованих на запобігання загрозам економічній безпеці підприємництва, припускає аналіз гіпотетичного (прогнозованого) стану підприємницького середовища внаслідок виконання прийнятих раніше стратегічних економічних і науково-технічних рішень, загальних тенденцій і процесів, які стосуються потрібності продукції і послуг, інвестицій тощо.

Узагальнюючи наведене, можна зробити висновок, що перехід України від однієї системи державного управління до іншої, на жаль, супроводжується

суттєвими кризами в економіці країни та суспільно-політичному житті, що часто руйнує сприятливі передумови для активізації підприємницької діяльності населення та розвитку підприємництва загалом. Загрози та ризики, які з'являються у перехідний період, можуть чинити непереборні труднощі щодо становлення і розвитку підприємництва. Посилення будь-якої із перерахованих нами вище загроз призводить до дестабілізації виробничих, комерційних зв'язків, нестабільної ситуації на ринку тощо. Проведені у дослідженні класифікації ризиків дозволяють деталізувати види і джерела загроз, більш системно підходити до їх передбачення та прогнозування наслідків негативного впливу, визначати структуру ризиків, а також врахувати можливість появи системних ризиків підприємництва, що можуть чинити загрозу не лише його розвитку, але й функціонуванню як сфери діяльності.

7.2 Дослідження ризиків та загроз економічній безпеці у всіх сферах діяльності підприємства

Для проведення аналізу впливу ризиків та загроз у фінансово-економічній безпеці на фінансово-господарську діяльність підприємства доцільно передусім згрупувати їх за джерелами: напрямом діяльності; етапами технологічного процесу; ресурсним забезпеченням та етапами життєвого циклу підприємства.

Класифікація джерел загроз економічній безпеці підприємства

1. Етап технологічного процесу:
- замовлення товарних (виробничих) запасів;
- транспортування;
- розвантаження, складування;
- внутрішньологістичні процеси;
- встановлення ціни, мерчендайзинг;
- реалізація товарів

2. Ресурсне забезпечення підприємства:
- оборотні активи;
- необоротні активи;
- персонал;
- нематеріальні активи;
- інформація

3. Напрям діяльності підприємства:
- маркетинговий;
- фінансово-економічний;
- інноваційний;
- комерційний;
- матеріально-ресурсне забезпечення;
- соціальний

4. Етап життєвого циклу підприємства:
- створення;

– започаткування діяльності;
– розвиток;
– зрілість;
– спад;
– диверсифікація діяльності

У межах кожного з цих джерел виникають загрози погіршення життєздатності підприємства чи його функціональних складових, що потребує їх моніторингу та управління. Тому необхідно окреслити завдання і принципи забезпечення економічної безпеки підприємства, відповідно до загроз його фінансово-господарській діяльності. Джерела загроз, завдання і принципи забезпечення фінансово-економічної безпеки підприємства наведені в табл. 7.3.

Таблиця 7.3

Джерела загроз, завдання і принципи забезпечення фінансово-економічної безпеки підприємства

Фактори	**Джерело загрози**	**Головні завдання**	**Пріоритетні принципи**
1	**2**	**3**	**4**
Залежно від етапу життєвого циклу підприємства	Діяльність пов'язана зі створенням підприємства та започаткуванням його функціонування	Раціональне планування цехового та складського господарства, налагодження системної сукупності зв'язків із постачальниками	Прогнозованості при проходженні етапів життєвого циклу; ціле встановлення та визначення місії.
	Фінансово-господарська діяльність	Формування ефективної логістичної системи постачання, забезпечення фінансової безпеки, розробка ефективної та дієвої конкурентної стратегії	Плановості, керованості та поступальності у розвитку
	Господарська діяльність на етапі зрілості	Створення ефективної системи моніторингу і планування діяльності, реалізація превентивних заходів безпеки	Адаптивності до змін ринкового середовища, попиту; підвищення рівня реакції на зміни зовнішнього середовища
	Функціонування на етапі спаду	Пошук можливостей вертикального та горизонтального розширення напрямів і видів діяльності, використання ресурсного забезпечення, підвищення рівня використання економічного потенціалу	Диверсифікації діяльності; оптимізації ресурсного забезпечення
	Діяльність, пов'язана з	Припинення діяльності з найменшими витратами,	Припинення діяльності після виконання місії та

Продовження таблиці 7.3

1	2	3	4
	диверсифікацією або перепрофілюванням діяльності	пошук нових видів економічної діяльності та переміщення в них капіталу	цілей і проходження етапів життєвого циклу
У межах напрямів діяльності підприємства	Маркетингова діяльність	Дослідження ринку та цільових сегментів, розробка та використання ефективних заїздів товароруху, обґрунтування цінової політики, стимулювання попиту,раціоналізація асортиментної політики, належного сервісного обслуговування	Безперервності, оперативності, науково-інформаційної обґрунтованості політки
	Фінансова діяльність	Забезпечення високого рівня ділової активності, платоспроможності та ліквідності, стійкого фінансового стану і належного рівня доступу до фінансових та інвестиційних ресурсів	Оперативності, обґрунтованості політики
	Інноваційна діяльність	Формування ефективності інноваційно-інвестиційної політики, впровадження технічних, організаційних та інших нововведень	Економічної доцільності та ефективності політики
	Комерційна діяльність	Активний пошук ринків збуту, потенційних споживачів, налагодження тривалих зв’язків з ними	Обґрунтованості
За групами ресурсного забезпечення	Використання оборотних активів	Забезпечення необхідних обсягів оборотного капіталу, ефективне використання оборотних коштів у часі	Високої швидкості обертання; повноцінності нормування
	Використання необоротних активів	Ефективне і раціональне використання виробничих приміщень та матеріально-технічної бази	Капіталізація підприємства; забезпечення активності та оновлення необоротного капіталу

Продовження таблиці 7.3

1	2	3	4
	Використання персоналу	Укомплектування необхідною кількістю кваліфікованого персоналу, формування належної системи стимулювання працівників	Оптимізації структури персоналу; високого рівня укомплектованості та кваліфікації, стабільності персоналу
	Використання нематеріальних активів	Систематичний пошук, реалізація інноваційної моделі, використання нематеріальних чинників підвищення конкурентоспроможності підприємства	Високого рівня захищеності прав власності; інноваційності типу господарювання
Під час проходження етапів технологічного процесу	Замовлення товарних чи виробничих запасів	Вивчення попиту, формування надійних зв'язків із постачальниками	Плановості, своєчасності та повноти поставок
	Транспортування	Своєчасне повне й ритмічне забезпечення товарно-виробничими запасами в належному асортименті, забезпечення ефективності логістичних процесів	
	Розвантаження товарів	Швидкість та оперативність навантажувально-розвантажувальних робіт	Оптимізації процесів навантажувально-розвантажувальних робіт
	Встановлення ціни, маркетингова діяльність	Узгодженість інтересів конкурентності та економічної обґрунтованості цінової політики,	Науковості ціноутворення; стратегічного підходу до процесу ціноутворення; оптимальності маркетингової діяльності
	Збут продукції	Забезпечення зручності та економічної ефективності збутового процесу, надання додаткових послуг споживачам	Оперативності; ритмічності поставок

Загалом дотримання визначених нами принципів та виконання завдань дасть змогу протистояти негативним впливам зовнішнього середовища та є

основою для створення повноцінного механізму забезпечення фінансово-економічної безпеки.

Для аналізу рівня фінансово-економічної безпеки підприємства доцільно виділяти такі рівні ризиків підприємницької діяльності:

1. Неризикова зона (підприємство функціонує стабільно, існують резерви для динамічного розвитку підприємства).

2. Зона припустимого ризику (підприємство ризикує втратити балансовий прибуток).

3. Зона критичного ризику (підприємство ризикує втратити виручку від реалізації продукції).

4. Зона катастрофічного ризику (підприємство ризикує втратити все своє майно).

Для виявлення й оцінювання рівня загроз фінансовій безпеці підприємства найбільш придатні такі методи аналізу: SWOT-аналіз, PEST-аналіз,SNW-аналіз, метод розробки сценаріїв розвитку подій. Розглянемо особливості їх застосування при виявленні й оцінюванні рівня загроз фінансовій безпеці підприємства.

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

У нашому випадку сильними сторонами фінансової діяльності підприємства виступають позитивні внутрішні умови здійснення фінансової діяльності, слабкими сторонами – негативні внутрішні умови у вигляді внутрішніх загроз, можливостями – позитивні зовнішні умови здійснення фінансової діяльності, власне загрозами – негативні зовнішні чинники у вигляді зовнішніх загроз фінансовій безпеці.

При застосуванні SWOT-аналізу в процесі виявлення і визначення рівня загроз фінансовій безпеці слід мати на увазі, що найсуттєвіші загрози виникають тоді, коли негативний розвиток ситуації у зовнішньому середовищі підприємства накладається на слабкі сторони самого механізму управління ФБП, тобто у такому разі виникає негативний кумулятивний ефект. Найбільші потенційні можливості забезпечення належного рівня ФБП стають результатом наявності і сукупної дії позитивних чинників зовнішнього середовища і сильних сторін самого механізму управління фінансовою безпекою.

Використання SWOT-аналізу надає можливість також визначати стратегії дій щодо забезпечення фінансової безпеки підприємства. Для цього слід застосовувати відповідну матрицю (рис. 7.1).

На перетинах виявлених груп чинників формуються поля, які надають можливість обирати (розробляти) відповідну стратегію забезпечення ФБП.

Для цих полів характерні такі поєднання і типи стратегій:

1) *поле ВСС-ЗМ* – на цьому полі поєднуються внутрішні сильні сторони механізму управління фінансовою безпекою і позитивні зовнішні чинники. Тому цьому полю має відповідати стратегія підтримки і розвитку сильних

сторін механізму управління ФБП у напрямі реалізації на конкретному підприємстві позитивних можливостей зовнішнього середовища;

2) *поле ВСлС-ЗМ* – на цьому полі поєднуються внутрішні слабкі сторони механізму управління ФБП з позитивними можливостями зовнішнього середовища. Тому це поле вимагає розробки і реалізації стратегії, яка має бути спрямована на подолання слабких сторін механізму управління ФБП підприємства за рахунок можливостей, які надає для нього зовнішнє середовище;

3) *поле ВСС-ЗЗ* – поряд із внутрішніми сильними сторонами механізму управління ФБП наявні і загрози з боку зовнішнього середовища. У такому разі потрібна стратегія використання сильних внутрішніх сторін для можливого подолання негативних впливів з боку зовнішнього середовища;

4) *поле ВСлС-ЗЗ* – «кризове поле», на якому поєднуються внутрішні слабкі сторони механізму управління ФБП із зовнішніми загрозами. У такому випадку необхідна стратегія, яка має бути спрямована як на подолання зовнішніх загроз, так і на усунення слабких місць у механізмі управління фінансовою безпекою, тобто внутрішніх негативних чинників.

		Зовнішнє середовище	
		Можливості 1 2 …	Загрози 1 2 …
Внутрішнє середовище	Сильні сторони 1 2 …	Поле ВСС-ЗМ	Поле ВСС-ЗЗ
	Слабкі сторони 1 2 …	Поле ВСлС-ЗМ	Поле ВСлС-ЗМ

Рис. 7.1 Матриця використання SWOT-аналізу для виявлення і якісного оцінювання рівня загроз фінансовій безпеці

Для виявлення і якісного оцінювання рівня загроз фінансовій безпеці підприємства можна використовувати метод PEST-аналізу, який дозволяє виявляти загрози з боку зовнішнього середовища макрорівня.

Згідно з цим методом, такі загрози поділяють на чотири різновиди, які позначаються абревіатурою англійських літер PEST:

P (political and legal environment) – політико-правове середовище;

E (economic environment) – економічне середовище,

S (sociocultural envirionment) – соціокультурне середовище,

T (technological envirionment) – технологічне середовище.

У політико-правовому середовищі на рівень фінансової безпеки підприємства у перспективі впливають чинні форми і методи державного регулювання:

1) всіх фінансових ринків;

2) політика бюджетної підтримки окремих галузей і підприємств;

3) державна політика підготовки кваліфікованих фахівців;

4) політика залучення і захисту іноземних інвестицій;

5) законодавче регулювання процедур фінансової санації та банкрутства;

6) державні стандарти фінансової звітності підприємств.

Економічне середовище впливає і, відповідно, приховує загрози фінансовій безпеці підприємства через ті чи інші темпи розвитку економіки країни. Насамперед це стосується ВВП, національного доходу, темпів інфляції, балансу грошових доходів і витрат населення, динаміки валютного курсу, рівня кредитних ставок, рівня монетизації економіки, облікової ставки НБУ, наявності дефіциту державного бюджету, сальдо зовнішньоторговельного балансу тощо.

У соціокультурному середовищі на стан фінансової безпеки підприємства впливають чинники, які можуть мати негативний характер: освітній і культурний рівень працездатного населення, рівень підготовки фахівців з вищою освітою в галузі фінансової діяльності, ставлення населення до здійснюваних ринкових реформ.

Технологічне середовище найбільше впливає на стан фінансової безпеки через впровадження інновацій у технічні засоби управління, фінансові інструменти і технології.

У процесі проведення PEST-аналізу спочатку виявляються зовнішні загрози, а потім оцінюється їхній вплив на стан фінансової безпеки підприємства.

Рівень впливу позитивних або негативних чинників (загроз), дія яких відображається на рівні фінансової безпеки підприємства, за цим методом може оцінюватися за п'ятибальною системою. При цьому оцінка нейтральної позиції приймається за нульову. Ця позиція, як правило, відповідає середньогалузевим значенням того чи іншого чинника впливу (загрози) на рівень фінансової безпеки на аналогічних підприємствах. Такий підхід надає можливість вважати нейтральну позицію пороговим значенням рівня фінансової безпеки підприємства, мінімальним її рівнем, після якого підприємство опиняється у небезпечному фінансовому стані.

Тоді інші значення позиції будуть такими:

-2 – дуже низька позиція (стан фінансової безпеки), близька до банкрутства;

-1 – низька позиція;

0 – нейтральна позиція (пороговий або мінімальний рівень фінансової безпеки);

+1 – достатньо безпечна позиція;

+2 – абсолютно безпечна позиція.

За результатами якісної оцінки впливу внутрішніх загроз фінансовій безпеці підприємства складається матриця сильних і слабких позицій підсистеми забезпечення ФБП (табл. 7.4). У вигляді сукупності напрямків забезпечення фінансової безпеки використано перелік домінантних сфер загальної стратегії, наведений в працях І.А. Бланка і М.М. Єрмошенко стосовно обраного об'єкта дослідження – фінансової безпеки підприємства. При цьому оцінюється кожен наведений у табл. 1 чинник і виставляється оцінка за п'ятибальною системою: від -2 до +2 (як було показано вище).

У науковій літературі відомо декілька формул для кількісного визначення розміру збитку від дії загроз. Так, В.В. Шликов пропонує застосовувати для цього коефіцієнт збитку *Ку*, який він обчислює за формулою:

$$K_y = ДВВ / Q_c \qquad (1)$$

де Q_c – обсяг власних ресурсів;

ДВВ – дійсна величина втрат, яка обчислюється за формулою:

$$ДВВ = ФЗ + ЗЗЗ + ЗВЗ \qquad (2)$$

де ФЗ – фактичні збитки;

ЗЗЗ – затрати на зниження збитків;

ЗВЗ – затрати на відшкодування збитків.

Таблиця 7.4

Матриця результатів проведення SNW-аналізу стану фінансової безпеки підприємства

Напрями забезпечення фінансової безпеки підприємства і чинники, які аналізуються	Позитивні внутрішні чинники впливу на стан ФБП (оцінка)		Негативні внутрішні чинники (загрози) впливу на стан ФБП (оцінка)	
	Коротко строві	Довго строкові	Коротко строві	Довго строкові
1	2	3	4	5
І. Забезпечення росту дохідності власного капіталу підприємства				
1.1 Тривалість операційного циклу підприємства				
1.2 Методи ціноутворення на реалізовану продукцію				
1.3 Співвідношення постійних і перемінних витрат				
1.4 Сукупність використовуваних підприємством податкових пільг				
ІІ. Формування фінансових ресурсів підприємства				
2.1 Рівень капіталізації чистого прибутку підприємства				
2.2 Методи амортизації активів, які використовуються підприємством				
2.3 Рівень кредитоспроможності підприємства				
2.4 Швидкість обороту капіталу				
ІІІ. Забезпечення фінансової стабільності підприємства				
3.1 Структура капіталу підприємства				
3.2 Структура активів капіталу				

Продовження таблиці 7.4

1	2	3	4	5
3.3 Збалансованість і синхронність окремих видів грошових потоків підприємства				
3.4 Розмір і склад поточних фінансових зобов'язань підприємства				
3.5Співвідношення дебіторської та кредиторської заборгованості підприємства				
3.6 Забезпеченість підприємства сласними оборотними активами				
3.7 Тривалість фінансового циклу підприємства				
IV. Забезпечення підприємства інвестиційними ресурсами				
4.1 Рівень задоволеності інвестиційних потреб підприємства				
4.2 Співвідношення обсягів реального і фінансового інвестування				
4.3 Склад реальних інвестиційних проектів підприємства, що реалізуються, за рівнем доходності				
4.4 Сукупність інструментів портфеля фінансових інвестицій підприємства за рівнем дохідності				
V. Нейтралізація фінансових ризиків підприємства				
5.1 Рівень диверсифікації фінансової діяльності і фінансових операцій підприємства				
5.2 Склад і розміри страхових фондів підприємства				
5.3 Склад кредитного портфеля підприємства за рівнем ризику				
VI. Інноваційне забезпечення діяльності підприємства				
6.1 Склад використовуваних підприємством фінансових інструментів і технологій та їх відповідність сучасному інноваційному рівню				
6.2 Рівень ефективності чинної організаційної структури фінансового менеджменту				
6.3 Рівень організаційної структури фінансових менеджерів підприємства				
6.4 Якість інноваційного менеджменту на підприємства				
VII. Антикризове управління підприємством				
7.1 Можливості скорочення фінансових потреб підприємства				
7.2 Можливості припинення неефективних видів				
7.3 Рівень фінансової безпеки операційної діяльності підприємства				
7.4 Якість антикризового управління підприємством				

Погоджуючись із наведеними формулами, слід зауважити, що вони не враховують імовірність самої загрози. Тому краще у кількісному виразі

визначати рівень самої загрози через розмір збитку від дії конкретної загрози фінансовій безпеці підприємства разом з імовірністю здійснення цієї загрози.

Це можна виразити такою математичною формулою:

$$P_{ФБП} = З_{ФБП} \times I_З \quad (3)$$

де $Р_{ФБП}$ – рівень загрози фінансовій безпеці підприємства; $З_{ФБП}$ – розмір збитку від дії загрози; $I_З$ – імовірність настання загрози.

Розмір збитку від дії загрози доцільно розраховувати за формулою (2).

Останній показник визначається експертним шляхом.

Після визначення загроз й оцінювання рівня їх впливу на рівень фінансової безпеки підприємства постає завдання їх нейтралізації.

Шляхами впливу з боку підсистеми управління фінансовою безпекою підприємства на нейтралізацію загроз можуть бути:

1) профілактика загроз, тобто зниження ризику виникнення загрози;

2) пом'якшення можливих наслідків від реалізації загроз.

7.3 Методологія діагностування ризиків, загроз та небезпек, їх оцінка та мінімізація

Діагностика – це певний набір методичних розробок, який дозволяє на ранніх стадіях визначити кризові ситуації, оцінити ступінь їх загрози для суб’єктів підприємництва та фактори, що їх викликали.

Завдання, що поставлені перед діагностикою:

1. Аналіз внутрішнього та зовнішнього середовища суб’єкта підприємництва.

2. Визначення кризового середовища і виділення критичних ризиків.

3. Оцінка ймовірності настання криз та можливості банкрутства.

4. Виділення проблемних місць у роботі суб’єкта підприємництва спираючись на дані проведеного аналізу.

5. Оцінка ефективності діяльності суб’єкта підприємництва.

Види діагностики у фінансово-економічній діяльності підприємства:

– *фундаментальна діагностика*, яка включає:

А. Визначення стадії життєвого циклу підприємства;

Б. Ідентифікацію критичних ризиків;

В. Комплексний аналіз з використанням коефіцієнтів;

С. Якісний аналіз діяльності підприємства.

– *комплексна діагностика:*

А. Комплексний аналіз з використанням коефіцієнтів;

Б. Якісний аналіз діяльності підприємства.

– *Експрес-діагностика:*

А. Проведення тест-анкетуванння.

Розглянемо методику проведення кожного виду діагностики:

1. *Експрес-діагностика* проводиться раз на місяць шляхом заповнення тестової анкети, побудованої з застосуванням якісних показників. За кожним

критерієм виставляються бали від 0 до 10 залежно від ступеня його реалізації на підприємстві (табл. 7.5).

2. *Комплексна діагностика* проводиться щоквартально із використанням розширеної тестової анкети, в яку входить 20 критеріїв оцінки (табл. 7.6).

3. *Фундаментальна діагностика* проводить один раз на рік у період підготовки річного звіту. Її основою є комплексна діагностика, але вона більш детально характеризує критичні ризики підприємства та якісні критерії.

Таблиця 7.5

Тестова анкета для щомісячної діагности фінансової безпеки підприємства (експрес-діагностика)

Критерії	Максимальна оцінка
1. Погані фінансові показники, наприклад, значення окремих статей фінансових звітів	10
2. Проведення «авральних заходів», збільшення залучених коштів, зниження заробітної плати, згортання перспективних програм	10
3. Небезпечні не фінансові системи, наприклад, прогрішення якості продуктів і послуг, морального духу персоналу	10
4. Зриви у виконанні зобов'язань	10
5. Перевищення деякого критичного рівня кредиторської заборгованості	10
6. Надмірне використання короткострокових позикових коштів як джерела фінансування довгострокових вкладень	10
7. Невиконання зобов'язань перед інвесторами, кредиторами тощо	10
8. Втрата ключових контрагентів	10
9. Зниження обсягів продажів	10
10. Втрата ключових співробітників апарату управління	10
11. Максимум загальної оцінки	100
12. Небезпечний рівень загальної оцінки	25

Розглянемо основні форми діагностування небезпек, загроз та ризиків, які впливають на фінансово-економічну діяльність підприємства з боку різних економічних структур.

Органи державного управління:

– зміна законодавства;
– корупційні дії;
– «співпраця» влади з конкурентами;
– бюрократичні перепони при проходженні дозвільних процедур;
– збільшення податкового тиску;
– підвищення мінімальної заробітної плати та відрахувань на соціальні заходи;
– введення жорстких технічних вимог;
– ускладнення амортизаційної політики.

Споживачі:

– істотна зміна смаків та уподобань;
– зниження купівельної спроможності;
– об'єднання в групи з метою впливу на рівень цін;

– крадіжки;

– використання недосконалості законодавства про захист прав споживачів з корисливою метою;

– поширення неправдивої інформації про підприємство та його товари.

Таблиця 7.6

Тестова анкета для комплексної діагности фінансової безпеки підприємства

Критерії	Максимальна оцінка
1. Погані фінансові показники, наприклад, значення окремих статей фінансових звітів	10
2. Проведення «авральних заходів», збільшення залучених коштів, зниження заробітної плати, згортання перспективних програм	10
3. Небезпечні не фінансові системи, наприклад, прогрішення якості продуктів і послуг, морального духу персоналу	10
4. Зриви у виконанні зобов'язань	10
5. Перевищення деякого критичного рівня кредиторської заборгованості	10
6. Надмірне використання короткострокових позикових коштів як джерела фінансування довгострокових вкладень	10
7. Невиконання зобов'язань перед інвесторами, кредиторами тощо	10
8. Втрата ключових контрагентів	10
9. Зниження обсягів продажів	10
10. Втрата ключових співробітників апарату управління	10
11. Хронічна недостача оборотних коштів	10
12. Висока питома вага простроченої дебіторської заборгованості	10
13. Застосування у виробничому процесі устаткування з простроченими термінами експлуатації	10
14. Несприятливі зміни в портфелі замовлень	10
15. Недостатня диверсифікованість діяльності підприємства	10
16. Політичний ризик, пов'язаний з підприємством в цілому чи його ключовими розділами	10
17. Різке зменшення коштів на рахунках	10
18. Розбалансування дебіторської та кредиторської заборгованості	10
19. Конфлікти на підприємстві, звільнення керівника тощо	10
20. Недостатнє технічне та технологічне відновлення підприємства	10
21. Максимум загальної оцінки	200
22. Небезпечний рівень загальної оцінки	50

Постачальники:

– навмисні недобросовісні конкурентні дії;

– невиконання умов поставок;

– розірвання контракту;

– одностороння зміна (невиконання) умов договору;

– непередбачуване збільшення цін на товари та витрат на їх постачання;

– постачання неякісних товарів або таких , які не відповідають стандартам і нормам;

– нездатність забезпечення підприємства новими конкурентоспроможними товарами.

Конкуренти:

– агресивна конкурентна політика збільшення ринкової частки (у т.ч. за рахунок розвитку роздрібної мережі);

– недобросовісна конкурентна поведінка;

– встановлення економічно не виправданих низьких цін;

– «співпраця» конкурентів із органами влади, спрямована на ускладнення доступу до ринку та господарських ресурсів для інших суб'єктів;

– переманювання персоналу;

– впровадження технічних інновацій;

– монополізація зв'язків із постачальниками.

Методичні підходи до оцінки рівня економічної безпеки повинні характеризувати її існуючий рівень, враховувати та відображати ймовірність настання небажаних негативних впливів та загроз внутрішнього та зовнішнього середовищ підприємства. Високий рівень економічної безпеки досягається лише за умови, що вся сукупність показників перебуває в межах гранично допустимих значень. В свою чергу, методологія оцінки рівня економічної безпеки підприємств повинна охоплювати перелік критеріїв та індикаторів (з конкретними числовими пороговими значеннями), а також передбачати поєднання таких методів дослідження як моніторинг соціально-економічних показників, експертних оцінок, багатовимірного статистичного аналізу.

7.4 Проведення контролю та оцінки рівня фінансово-економічної безпеки на підприємстві

Контролем визначається процес забезпечення досягнення підприємством своїх цілей, за допомогою якого керівники досягають відповідності фактичних дій із запланованими.

Метою системи контролю – є своєчасне виявлення відхилень від нормального – запланованого перебігу провадження та здійснення адекватних управлінських заходів щодо покращання становища для забезпечення виконання розроблених планів. Досягнення встановлених цілей діяльності.

Під оцінкою будемо розуміти співвідношення об'єкта з прийнятим критерієм, взірцем чи нормою. Ці дві підсистеми взаємопов'язані між собою.

В системі фінансово-економічної безпеки виділяють три ключові складові діяльності підсистеми контролю та оцінки:

1. Методологічна складова – розробка методології оцінки рівня фінансової безпеки, участь у розробці антикризової програми;

2. Безпосередньо контроль – забезпечення достовірності даних від інших підсистем, контроль за виконанням підсистемами поставлених перед ними завдань;

3. Аналітична частина – обмін інформаційними потоками, аналіз змісту інформаційних потоків, аналіз відхилень, виявлення причин кризових ситуацій, надання рекомендацій керівнику.

У рамках дії системи фінансово-економічної безпеки підприємств здійснюють два типи контролю:

1. Поточний – здійснюється безпосередньо під час функціонування суб'єкта підприємництва та виконання антикризових заходів. Його головною метою є відстеження відповідності фактичних результатів до поставлених завдань, а також оцінюється ступінь ефективності дій щодо забезпечення фінансової безпеки;

2. Підсумковий – здійснюється за фактом закінчення звітного періоду чи реалізації комплексу антикризових заходів. Його мета – перевірка відповідності досягнутих результатів поставленим цілям, а також оцінка ефективності розпочатих заходів та ухвалення рішення про необхідність додаткових заходів щодо забезпечення фінансово-економічної безпеки.

Розглянемо комплекс контролю для забезпечення фінансово-економічної безпеки підприємства.

1. Підсистема контролю та оцінки результатів:
- контроль за виконанням підсистемою своїх функцій;
- оцінка результативності заходів з нейтралізації кризи;
- забезпечення обміну інформаційними потоками

2. Об'єкти дії підсистеми контролю:

2.1. Діяльність
- антикризові заходи;
- поточна діяльність суб'єкта підприємництва.

2.2.Результати:
- висновки підсистеми діагностики;
- результати антикризових заходів;
- результати діяльності суб'єкта підприємництва за певний період.

Всі управлінські рішення в галузі забезпечення захисту фінансових інтересів підприємства від зовнішніх і внутрішніх загроз найтіснішим чином взаємопов'язані і здійснюють прямий або опосередкований вплив на результати його фінансової діяльності.

Головна мета управління фінансово-економічною безпекою підприємства (ФЕБП) – забезпечення його стійкого і максимально ефективного функціонування, створення високого потенціалу розвитку і зростання в майбутньому. Важливою складовою економічної безпеки підприємства є фінансова безпека.

У короткостроковому періоді мета і завдання управління ФЕБП повинні бути орієнтовані на стабілізацію його фінансового стану, при якому закладаються основи для майбутнього розвитку. У довгостроковому періоді мета і завдання системи фінансової безпеки повинні бути спрямовані на збереження найважливіших фінансових пропорцій, що забезпечують постійне зростання його ринкової вартості.

В системі фінансового менеджменту доцільно виокремити підсистему управління фінансовою безпекою підприємства, до основних цільових орієнтирів якої слід віднести:

– забезпечення сталого економічного розвитку підприємства, досягнення основних цільових параметрів діяльності при збереженні ліквідності та певного рівня фінансової незалежності, необхідних для підтримки його стійкості в поточному періоді;

– нейтралізація негативного впливу кризових явищ економіки, навмисних дій конкурентів та інших «недружніх» структур;

– формування адекватної системи обліку фінансових потоків і підвищення ефективності системи контролю;

– залучення і використання позикових коштів за оптимальною вартістю;

– контроль прийнятного рівня боргового навантаження;

– запобігання випадкам халатності, шахрайства, а також умисних дій персоналу у відносинах з контрагентами, а також іншим фінансовим порушенням;

– розробка та впровадження системи постійного моніторингу фінансового стану підприємства з метою раннього діагностування кризових явищ та ознак банкрутства.

Реалізація перелічених напрямів допоможе підприємству створити необхідний запас міцності фінансової системи, що сприятиме забезпеченню подолання кризових наслідків. Фінансово-економічна безпека є досить складною системою з певною структурою і механізмом відносин між її елементами. В основі системи ФЕБП лежить принцип суворо цільового використання фінансових ресурсів і забезпечення певних умов для швидкої та ефективної віддачі від збільшення вкладених коштів. Реалізація подібного принципу означає створення системи контролю не тільки за доцільністю і своєчасністю використання коштів, але й за рівнем їх окупності.

Управління фінансовою безпекою підприємства необхідно здійснювати у двох режимах:

1. в умовах стабільного існування підприємства;

2. в умовах нестабільного існування підприємства.

До функцій управління фінансово-економічною безпекою в умовах стабільного існування підприємства відносять:

1. Формування ефективних інформаційних систем, що забезпечують обґрунтування альтернативних варіантів управлінських рішень.

2. Проведення аналізу стану фінансової та економічної безпеки підприємства.

3. Розробка системи планування ФЕБП.

4. Створення системи внутрішнього контролю ФЕБП.

Стратегія управління фінансово-економічною безпекою підприємства в умовах нестабільного існування повинна включати такі складові:

– діагностика кризових ситуацій;

– поділ об'єктивних і суб'єктивних негативних впливів;

– визначення переліку заходів щодо запобігання загрозам ФЕБП;

– оцінка ефективності планованих заходів з точки зору нейтралізації негативних впливів;

– оцінка ефективності пропонованих заходів щодо усунення загроз ФЕБП.

Основні етапи процесу управління фінансово-економічною безпекою підприємства представлено на рис. 7.2.

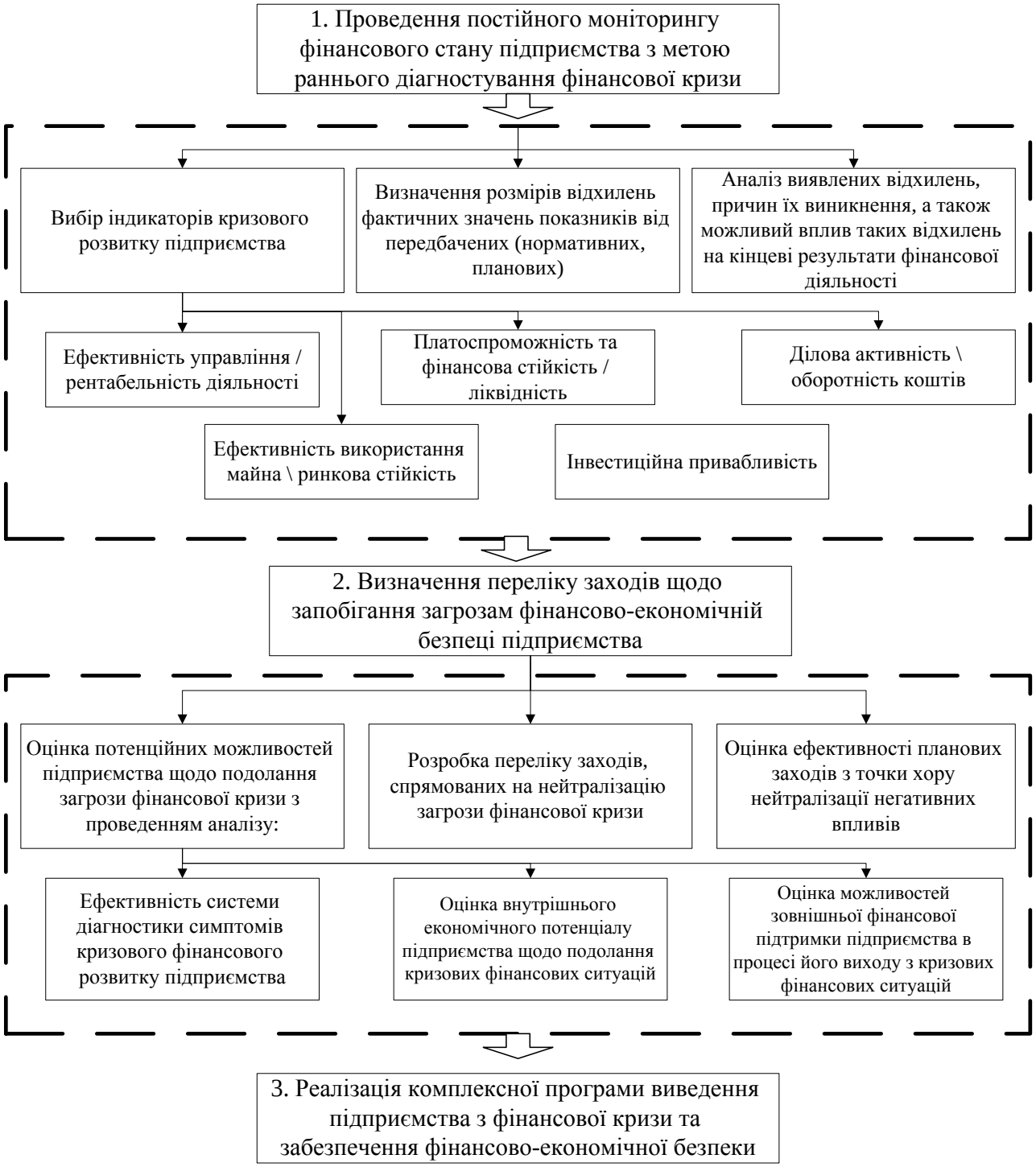

Рис. 7.2. Послідовність процесу управління фінансово-економічною безпекою підприємства

Залежно від результатів моніторингу фінансового стану підприємства з метою раннього діагностування фінансової кризи та забезпечення ФЕБП диференціюються напрями дій і розробляються антикризові заходи.

Комплекс заходів може бути спрямований на запобігання фінансовій кризі або на пом'якшення умов її майбутнього протікання, якщо в силу активного впливу факторів зовнішнього середовища запобігти фінансовій кризі не представляється можливим. Комплексний план заходів щодо запобігання загрозам фінансовій безпеці містить такі основні розділи:

– перелік антикризових заходів;

– обсяг фінансових ресурсів, що виділяються для їх реалізації; - терміни реалізації окремих антикризових заходів;

– очікувані результати фінансової стабілізації.

Основними заходами, спрямованими на нейтралізацію загрози фінансової кризи, є:

– страхування фінансових ризиків підприємства;

– реалізація зайвих або невикористовуваних активів підприємства;

– вжиття заходів щодо стягнення дебіторської заборгованості;

– скорочення обсягу фінансових операцій на найбільш ризикованих напрямках фінансової діяльності підприємства;

– економія інвестиційних ресурсів за рахунок призупинення реалізації окремих реальних інвестиційних проектів;

– економія поточних витрат, пов'язаних з господарською діяльністю підприємства;

– оцінка завантаження виробничих потужностей;

– передача об'єктів невиробничої сфери на баланс органів міської влади і скорочення витрат на їх утримання та ін.

Вибір заходів повинен бути спрямований на поетапне вирішення наступних завдань: усунення неплатоспроможності, щоб попередити виникнення процедури банкрутства; відновлення фінансової стійкості, що дозволить усунути загрозу відновлення фінансової кризи не тільки в короткому, але і в більш тривалому проміжку часу; забезпечення фінансової рівноваги в тривалому періоді.

Таким чином, зміст поняття фінансової безпеки можна визначити як граничний рівень його фінансового захисту від реальних та потенційних загроз зовнішнього і внутрішнього характеру, який визначається кількісними та якісними параметрами його фінансового стану, з урахуванням формування комплексу пріоритетних фінансових інтересів та створення системи необхідних фінансових передумов сталого розвитку в короткостроковому і довгостроковому періоді за умови постійного моніторингу фінансової безпеки і формування комплексу превентивних і контрольних заходів. Процес управління фінансово-економічною безпекою підприємства потребує розроблення відповідного механізму, компонентами якого є сукупність фінансових інтересів підприємства, організаційна структура й управлінський персонал, техніка і технологія управління, функції, принципи і методи управління, фінансові інструменти, критерії оцінки.

Метою моніторингу економічної безпеки підприємства є одержання інформації керівництвом підприємства про рівень ефективності і

результативності діяльності підприємства на основі якісного і кількісного аналізу і оцінювання відповідних показників та оцінки виникнення або існування можливих загроз та ризиків. Предметною областю моніторингу рівня економічної безпеки є визначення інтегрального показника економічної безпеки підприємства за виділеними функціональними складовими. Однією із умов, якою повинен відповідати алгоритм проведення моніторингу є можливість кількісної оцінки всіх досліджуваних показників для визначення рівня економічної безпеки промислового підприємства.

Моніторинг рівня економічної безпеки на підприємстві передбачає виконанні послідовних етапів регуляторного впливу.

На першому етапі відбувається формування системи економічної безпеки на підприємстві. Система регулювання економічної безпеки на підприємстві має наступні елементи: мета, завдання, об'єкт, суб'єкт, методи та інструменти. Метою регулювання економічної безпеки на підприємстві є визначення можливого стану системи економічної безпеки, яке може бути досягнуте за умови попередження виникнення загроз економічній безпеці та забезпечення розвитку людини і суспільства як пріоритетних. Спираючись на загальну методологію статистичного моніторингу та враховуючи особливості процесу підтримки належного рівня економічної безпеки підприємства при формуванні методичного підходу щодо здійснення внутрішнього моніторингу на підприємстві визначено наступні актуальні завдання:

– формування мети і основних завдань моніторингу рівня економічної безпеки, виходячи із місії, економічних завдань і інтересів, що стоять перед підприємством;

– формування системи одиничних показників-індикаторів, які можуть кількісно характеризувати стан окремих функціональних складових економічної безпеки підприємства;

– встановлення джерел інформації для проведення необхідних розрахунків рівня окремих функціональних складових економічної безпеки підприємства та інтегрального показника;

– збирання та передання для подальшої обробки необхідної інформації;

– оцінка достовірності та повноти і глибини надання інформації;

– зведення обробленої інформації у комп’ютерні бази даних;

– аналітична обробка інформації та отримання результатів щодо поточного рівня стану економічної безпеки підприємства;

– виявлення причин і наслідків низької ефективності функціонування системи регулювання економічної безпеки підприємства;

– розробка пропозицій з удосконалення регіонального регулювання для забезпечення безпеки;

– прогнозування рівня економічної безпеки підприємства.

Функції регулювання економічної безпеки на регіональному рівні забезпечуються принципами, методами, способами та інструментами управління економічною безпекою. Принципи управління визначають основні правила управлінської діяльності, які повинні виконуватися суб'єктами

управління. Під методами регулювання економічної безпеки розуміються способи впливу суб'єктів управління на об'єкти управління, основними серед які є: правові, адміністративні, економічні. При управлінні економічною безпекою підприємства використовуються наступні інструменти: законодавче та нормативно-правове забезпечення у сфері національної безпеки, державного та регіонального економічного управління; державне замовлення; соціальні норми і нормативи; критичні порогові значення економічних показників; державні дотації, субсидії, податкові пільги. Під способами регулювання розуміється дія або система дій, яка використовується для виконання забезпечення економічної безпеки на основі Закону України «Про основи національної безпеки України».

На другому етапі моніторингу регулювання економічної безпеки на підприємстві проводитися оцінка стану економічної безпеки регіону за виділеними функціональними складовими.

Дослідження стану економічної безпеки на підприємстві відбувається за основними функціональними складовими. За проведеним дослідженням виділено наступні функціональні складові економічної безпеки на підприємстві: фінансова, зовнішньоекономічна, інвестиційно-інноваційна, енергетична, кадрова, техніко-технологічна, екологічна, силова. Необхідно зауважити, що набір функціональних складових для кожного окремого підприємства може бути іншим. Відповідно, аналіз економічної безпеки регіону базується на наступній умові:

$$ЕБП = f\{ФБ; ЗЕБ; ІІБ; ЕнБ; КБ; ТТБ; ЕкБ; СБ\} \quad (4)$$

де ЕБП – економічна безпека підприємства; ФБ – фінансова безпека; ЗЕБ – зовнішньоекономічна безпека; ІІБ – інвестиційно-інноваційна безпека; ЕнБ – енергетична безпека; КБ – кадрова безпека; ТТБ – техніко-технологічна безпека; ЕКБ – екологічна безпека; СБ – силова безпека.

Основні етапи дослідження стану економічної безпеки підприємства наступні.

Перший етап. Формування системи одиничних показників вимірювання функціональних складових. Основою формування системи одиничних показників є ідея збалансованої системи показників [3]. У відповідності з цим підходом оцінка функціональної складової за допомогою системи збалансованих показників дозволяє в повному обсязі визначити стан складової економічної безпеки. Використання головної ідеї збалансованої системи показників полягає у формуванні положень стратегічно безпечного розвитку підприємства на основі визначеного в ході загальної оцінки рівня економічної безпеки і можливих загроз.

На другому етапі проводитися розрахунок одиничних показників економічної безпеки підприємства за формулами. Кожен одиничний показник має рекомендоване значення. Це дозволяє виділити індикатори, які не відповідають нормам, а також визначити негативні сторони розвитку.

На третьому етапі проводиться формування рівнянь бажаності за всіма одиничними показниками економічної безпеки. Оцінка рівня економічної безпеки підприємства передбачає приведення різних критеріїв її дослідження до єдиного універсального параметру, а саме до інтегральному показнику ЕБР. Під критерієм бажаності розуміється граничне кількісний вимір відносного значення конкретного одиничного показника. Який визначається за допомогою функції Харрінгтона.

На четвертому етапі розраховуються групові показники економічної безпеки підприємства за допомогою визначення середньо геометричного значення.

На п'ятому етапі розраховується інтегральний показник рівня економічної безпеки підприємства за функціональними складовими. Розрахований інтегральний показник рівня економічної безпеки підприємства узагальнює безліч одиничних показників і чисельно відображає відносну оцінку рівня її складових. Порівнюючи отриману величину інтегрального показника рівня економічної безпеки підприємства з діапазоном значень економічної безпеки у відповідності з теорією Харрінгтона, можна зробити висновки про рівень економічної безпеки підприємства.

Експертна система дозволяє провести оцінку рівня загроз економічній безпеці підприємства і провести їх ранжування. На цьому етапі особливо важливе значення має об'єктивна, повна і комплексна інформація про фінансово-економічний стан підприємства. Важливе значення має також інформація про ступінь реалізації пріоритетних інтересів підприємства в економічній, соціальній, інноваційній сферах, визначених на законодавчому рівні. Моніторинг передбачає процедуру аналізу економічної ситуації, виявлення тенденцій соціально-економічного, інноваційного та інвестиційного розвитку підприємства, оцінки рівня загроз економічній безпеці. На цьому етапі при розрахунку рівня економічної безпеки підприємства кожний окремий показник складових економічної безпеки порівнюється з граничним або пороговим значенням. Проблема підвищення рівня наукової обґрунтованості та адаптації до умов України порогових значень показників, визначених світовою практикою державного управління є актуальною, оскільки є певні розбіжності у величинах порогових значень показників. Формування алгоритму розрахунку інтегрального показника рівня економічної безпеки підприємства теж є важливою проблемою. Це викликано необхідністю відстеження наслідків економічних трансформацій в Україні з урахуванням вимог національної безпеки.

На третьому етапі моніторингу здійснюється оцінка можливостей регулювання забезпечення економічної безпеки підприємства. Для цього необхідно провести оцінку загроз, які знижують ефективність і якість функціонування підприємства та знижують рівень управління економічною безпекою. З'ясування причин неефективного регулювання економічною безпекою на рівні підприємства, дає можливість розробити певні заходи з приводу їх усунення. Якщо такі причини ліквідувати неможливо, то необхідно

розробити певні заходи щодо попередження виникнення можливих загроз, які знижують ефективність регулювання економічної безпеки.

Четвертий етап моніторингу – це розробка і впровадження інструментарію регулювання економічної безпеки на рівні підприємства, регіону та країни відповідно до Закону України «Про основи національної безпеки України» і на основі Стратегії забезпечення економічної безпеки регіону, якщо така стратегія була прийнята.

П'ятий етап моніторингу – це спостереження і контроль за виконанням попередніх етапів. Контроль повинен забезпечувати порівняння фактичного стану економічної безпеки підприємства з бажаним, націлений на своєчасне виявлення відхилень і встановлення їх причин; встановлення недоліків і помилок управлінської діяльності; спостереження за змінами соціально-економічної, інвестиційно-інноваційного середовища і прогнозування стану економічної безпеки підприємства. Одночасно контроль повинен мати форму зворотного зв'язку, на основі якої можна здійснювати координацію управління економічною безпекою.

Дієвість регулювання економічною безпекою на підприємстві залежить від ефективності функціонування підприємства. Результатом ефективного державного регулювання економічної безпеки на рівні регіону є реалізація державних і регіональних програм щодо забезпечення економічної безпеки і забезпечення зв'язків з громадськістю.

Процес моніторингу регулювання економічної безпеки підприємства складається з п'яти основних етапів: 1) формування системи економічної безпеки на підприємстві; 2) оцінки стану економічної безпеки підприємства за виділеними функціональними складовими; 3) оцінки можливостей регулювання забезпечення економічної безпеки підприємства; 4) розробки та впровадження інструментарію регулювання економічною безпекою підприємства, спостереження; 5) контролю за виконанням попередніх етапів.

Контрольні питання:

1. Сутність поняття «загроза» фінансово-економічної безпеки.
2. Параметри при визначені загроз.
3. Зовнішні загрози фінансово-економічної безпеки.
4. Джерела зовнішніх загроз фінансово-економічної безпеки.
5. Внутрішні загрози фінансово-економічної безпеки.
6. Джерела внутрішніх загроз фінансово-економічної безпеки.
7. Економічні загрози.
8. Виробничі загрози.
9. Правові ризики.
10. Класифікація загроз за частотою їх виникнення.
11. Економічні та фінансові загрози.
12. Об’єктивні та суб’єктивні загрози.
13. Реальні та потенційні загрози.

14. Функції органів державного управління при управління фінансово-економічної безпеки підприємства.
15. Класифікація джерел загроз фінансово-економічної безпеки на різних етапах діяльності підприємства.
16. Джерела загроз, завдання і принципи забезпечення фінансово-економічної безпеки.
17. Рівні ризику підприємницької діяльності.
18. Використання SWOT-аналізу при оцінці загроз фінансово-економічної безпеки.
19. Використання PEST-аналізу при оцінці загроз фінансово-економічної безпеки.
20. Використання SNW-аналізу при оцінці загроз фінансово-економічної безпеки.
21. Сутність діагностики та завдання, які поставлені перед нею.
22. Види діагностики при оцінці фінансово-економічної безпеки підприємства.
23. Сутність експерс-діагностки при оцінці загроз фінансово-економічної безпеки.
24. Сутність комплексної діагностики.
25. Характеристика фундаментальної діагностики при оцінці загроз фінансово-економічної безпеки.
26. Форми діагности небезпек, загроз та ризиків, які впливають на фінансово-економічну безпеку з боку різних економічних структур.
27. Проведення контролю та оцінки фінансово-економічної безпеки підприємства.
28. Основні складові політики контролю та оцінки фінансово-економічної безпеки підприємства.
29. Комплексний контроль для забезпечення фінансово-економічної безпеки.
30. Мета та завдання управління фінансово-економічної безпеки підприємства.
31. Етапи процесу управління фінансово-економічної безпеки підприємства.
32. Заходи щодо запобігання загрозам фінансово-економічної безпеки підприємства.
33. Етапи моніторингу фінансово-економічної безпеки підприємства.
34. Основні етапи оцінки фінансово-економічної безпеки підприємства.
35. Методологія діагностики рівня фінансово-економічної безпеки підприємства.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Абакумов В.М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони/ В.М. Абакумов// Форум права. 2012. № 4. С. 10-16. – Режим доступу: http://nbuv.gov.ua/UJRN/FP_index.htm_2012_4_3

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

3. Бланк И.А. Концептуальные основы финансового менеджмента. – К.: Ника-Центр, Эльга, 2003. – 448 с.

4. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми // Стратегічна панорама. – 1999. – № 1-2. – С. 127-133.

5. Васильців Т.Г. Фінансова безпека підприємства: місце в системі економічної безпеки та пріоритети посилення на посткризовому етапі розвитку економіки /Т.Г. Васильців, О.Р. Ярошко// Збірник науково-технічних праць Національного лісотехнічного університету України. -2011. – Вип. 21.2. – С. 132-136.

6. Вергун А.М. Особливості управління фінансово-економічною безпекою/А.М. Вергун, Т.М. Нефедова, І.О. Тарасенко// //[Електронний ресурс]/ International scientific journal. - 2015. - № 2. - С. 27-31. - Режим доступу: http://nbuv.gov.ua/UJRN/mnj_2015_2_7

7. Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі/Н.М. Волошина//Modern Information Technologies in the Sphere of Security and Defenñe. – 2010. - № 2(8). – С. 53-56.

8. Гетьман О.О. Економічна діагностика: навч. посібник для студ. вищ. навч. зал. / О.О. Гетьман, В.М. Шаповал. - К.: Центр навчальної літератури, 2007. - 307 с.

9. Городня Т.А. Економічна та фінансова діагностика / Т.А. Городня, І.П. Мойсеєнко. - К.: ППНВ, 2008. - 282 с.

10. Горячева, К. С. Механізм управління фінансовою безпекою підприємства [Текст] : автореферат дис. канд. екон. наук : 08.06.01 / К. С. Горячева ; Київський нац. ун-т технологій та дизайну. – К., 2006. – 17 с.

11. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.

12. Донець Л.І. Економічна безпека підприємства: навч. посібник / Л.І. Донець, Н.В. Ващенко. - К.: Центр учбової літератури, 2008. - 240 с.

13. Дяченко К.С. Методичні підходи до оцінки рівня економічної безпеки підприємств будівельної галузі/ К.С. Дяченко// Technology audit and production reserves – № 4/5(24), 2015. – С. 31-36.

14. Економічна безпека підприємств, організацій та установ / за ред. Л. Ортинського. - К.: Правова єдність, 2009. - 542 с.

15. Економічна безпека підприємства /[Електронний ресурс] – Режим доступу: http://elearn.nubip.edu.ua/mod/page/view.php?id=1451 – Назва з екрану.

16. Економічний аналіз і діагностика стану сучасного підприємства: навч. посібник / [Костенко Т.Д., Підгора Є.О., Рижиков В.С., Панков В.А., Герасимов А.А., Ровенська В.В.]. - К.: Центр навчальної літератури, 2005. – 368 с.

17. Євтушевська О.А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту /[Електронний ресурс] – Режим доступу: http://zt.knteu.kiev.ua/files/2015/5-6%20(82-83)/18.pdf

18. Єпіфанов А.О. Фінансова безпека підприємств і банківських установ: монографія / А.О. Єпіфанов, О.Л. Пластун, В.С. Домбровький. - Суми: ДВНЗ «УАБС НБУ», 2009. - 295 с.

19. Єрмошенко М.М., Горячева К.С. Фінансова складова економічної безпеки: держава і підприємство: Наук. монографія. – К.: Національна академія управління, 2010. – 232 с.

20. Жихор О.Б. Місце і роль фінансової розвідки у структурі економічної розвідки/ О.Б. Жихор, М.В. Харламова//[Електронний ресурс]/ Науковий вісник НЛТУ України. - 2013. - Вип. 23.14. - С. 121-126. - Режим доступу: http://nbuv.gov.ua/UJRN/nvnltu_2013_23.14_21

21. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» /[Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1702-18

22. Закон України «Про основи національної безпеки України» [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15

23. Івахненков С.В. Фінансовий контролінг: методи та інформаційні технології / С.В. Івахненков, О.В. Мелих. - К.: Знання, 2009. - 319 с.

24. Інформаційна потужність держави, як складова національної безпеки. [Електронний ресурс] – Режим доступу: http://propolis.com.ua

25. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навч. посібник / М. І. Камлик. - К. : Атіка, 2005. - 432 с.

26. Картузов Є.П. Вплив ризиків і загроз на стан фінансової безпеки підприємств/ Є.П. Картузов//Актуальні проблеми економіки. – 2012. – № 9 (135). – С. 115-124.

27. Клименко, Т. В. Основні елементи механізму забезпечення фінансової безпеки суб’єктів господарювання [Текст] / Т. В. Клименко // Вісник ЖДТУ. Серія: Економічні науки. – 2011. – № 4 (58). – С. 340–343.

28. Конспект лекцій з дисципліни «Технологія діяльності аналітиків з питань фінансово-економічної безпеки» для студентів спеціальності 8.18010014 „Управління фінансово-економічною безпекою” / Ж.С. Шило – Рівне: НУВГП, 2014, 49 с.

29. Конституція України від 28.06.1996 № 254к/96-ВР зі змінами та доповненнями / [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр

30. Концепція економічної безпеки України. Ін-т екон. Прогнозування / кер. проекту В.М. Геєць. - К., 1999. - 56 с.

31. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

32. Кримінальний кодекс України від 5.04.2001 № 2341-III /[Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14

33. Кузенко Т.Б. Класифікація методів оцінки економічної безпеки підприємства / Т.Б. Кузенко // Економіка і управління. - 2003. - № 4. - С. 70-77.

34. Куликов П.М. Економіко-математичне моделювання фінансового стану підприємства: навч. посібник / П.М. Куликов, Г.А. Іващенко. - Харків: Інжек, 2009. - 152 с.

35. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04. / О.В. Литвиненко. – К., 1997. – 18 с.

36. Манойло А.В. Проблемы и перспективы исследования информационно-психологических технологий разрешения международных конфликтов./А.В. Манойло//[Електронний ресурс] //Право и политика. – 2008. - №3. – С. 592-598. – Режим доступу: http://yurpsy.fatal.ru/files/stat/manoylo/07.htm.

37. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки /А.І. Марущак // Державна безпека України. – 2011. – № 21. – С. 92–95.

38. Матковський А.П. Забезпечення інформаційної безпеки у фінансовій сфері як елемент економічної безпеки держави/ А.П. Матковський// Проблеми інформатизації та управління.2010. – № 2(30). – С. 131-135.

39. Матюшко Н.Г. Завдання фінансово-економічної безпеки на підприємстві в контексті сталого розвитку /Н.Г. Матюшко, З.Я. Шацька//[Електронний ресурс] – Режим доступу: http://knutd.com.ua/our-publikation/533/683/6880/

40. Методологічні засади державного регулювання фінансово-економічного розвитку / Плескач В. Л., Кулик А. В. // Фінанси України. – 2009. – № 10. – С. 27.

41. Механізм забезпечення фінансової безпеки підприємства /[Електронний ресурс] – Режим доступу: http://pidruchniki.com/78246/finansi/mehanizm_zabezpechennya_finansovoyi_bezpeki_pidpriyemstva – Назва з екрану

42. Мец В.О. Економічний аналіз фінансових результатів та фінансового стану підприємства: навч. посібник / В.О. Мец. - К.: Вища школа, 2003. - 278 с.

43. Минаев Г.А. Безопаность организации: ученик / Г.А. Минаев. - К.: КНТ, 2009. - 440 с.

44. Моделювання економічної безпеки: держава, регіон, підприємство / [В.М. Геєць, М.О. Кизим, Т.С. Клебанова, Т.С. Черняк] // Науково- дослідний центр індустріальних проблем розвитку НАН України; В.М. Геєць (ред.). - Х.: ВД «ИНЖЭК», 2006. - 240 с.

45. Мойсеєнко, І. П. Механізм управління фінансово-економічною безпекою підприємства [Текст] / І. П.Мойсеєнко, О. О. Шолок // Науковий вісник НЛТУ України : збірник науково-технічних праць. – Львів : РВВ НЛТУ України. – 2011. − Вип. 21.02. – С. 141–146.

46. Мойсеєнко, І. П. Управління фінансово-економічною безпекою підприємства [Текст] / І. П. Мойсеєнко, О.М. Марченко. – Львів : ЛьвДУВС, 2011. – 380 с.

47. Новак В.О. Інформаційне забезпечення менеджиенту: навч. посібник. – К.: Кондор, 2007. – 462 с.

48. Новікова О.Ф., Покотиленко Р.В. Економічна безпека: концептуальне визначення та механізм забезпечення: монографія. - Донецьк: НАН України, 2006. - 408 с.

49. Обліково-аналітичне забезпечення економічної безпеки підприємства [Текст]: Конспект лекцій для магістрів спеціальності 071 «Облік і оподаткування» денної і заочної форм навчання/ укл. Н.С. Вавдіюк, Т.А. Талах. – Луцьк: Луцький НТУ, 2016. – 132 с.

50. Одинцов А.А. Економічна і інформаційна безпека підприємництва: учеб. пособие для вузов / А.А. Одинцов. - М: Академія, 2006. - 336 с.

51. Орєхова К.В. Механізм забезпечення фінансової безпеки держави/К.В. Орєхова//[Електронний ресурс]/ Фінансово-кредитна діяльність: проблеми теорії та практики. - 2014. - Вип. 1. - С. 131-146. - Режим доступу: http://nbuv.gov.ua/UJRN/Fkd_2014_1_18

52. Орлик О.В. Механізм управління фінансово-економічною безпекою підприємства та його основні складові/ О.В. Орлик// Фінансово-кредитна діяльність: проблеми теорії та практики. – 2015. – Вип. 2 (19). – С. 222-232. [Електронний ресурс] – Режим доступу: http://dx.doi.org/10.18371/fcaptp.v2i19.57391

53. Осовська Г.В. Менеджмент організацій: підручник для студ. вищ. навч. закладів / Г.В. Осовська, О.А. Осовський. - К.: Кондор, 2009. - 680 с.

54. Поздняков В.Я. Анализ и диагностика финансово-хозяйственной деятельности предприятий: учебник для вузов / В.Я. Поздняков. - М.: ИНРФРА-М, 2010. - 617 с.

55. Постанова Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/3/97-вр

56. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах/ М.М. Присяжнюк, Я.С. Бєлошнвич// Вісник Київського національного

університету імені Тараса Шевченка / Київський національний університет імені Тараса Шевченка. – Київ, 2013. – С. 37-41.

57. Реверчук Н.Й. Управління економічною безпекою підприємницьких структур: монографія / Н.Й. Реверчук. - Львів: ЛБІ НБУ, 2004. - 195 с.

58. Руснак Л. Р. Сфера ризиків та загроз економічній безпеці суб'єктів підприємницької діяльності в Україні/Л.Р. Руснак, І.М. Ковальська // [Електронний ресурс] – Режим доступу: http://int-konf.org/konf122013/626-rusnak-l-r-kovalska-m-sfera-rizikv-ta-zagroz-ekonomchny-bezpec-subyektv-pdpriyemnickoyi-dyalnost-v-ukrayin.html

59. Садчикова І.В. Концептуальні засади інформаційно-аналітичного забезпечення фінансово-економічної безпеки підприємства / І.В. Садчикова, В.С. Садчиков//[Електронний ресурс] //Фінансові дослідження. -2016. - № 1 (1). - Режим доступу: http://fr.stu.cn.ua/

60. Світлична В.Ю. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення/ В.Ю. Світлична, Т.І. Світлична// http://economy.kname.edu.ua/images/files/publishing/360-369_Світлична_2.pdf

61. Система фінансового моніторингу /[Електронний ресурс] – Режим доступу: http://posibniki.com.ua/post-sistema-finansovogo-monitoringu – Назва з екрану.

62. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2/032-035.pdf.

63. Соснин А.С., Пригунов П.Я. Менеджмент безопасности предпринимательства. Учебное пособие. – К. Издательство Европейского университета, 2002 – 504 с.

64. Соснін О.В. Інформаційна політика України: проблеми розбудови [Електронний ресурс] – Режим доступу: http://www.niisp.gov.ua/vydanna/panorama

65. Соціально-економічна безпека: навч. посібник. К.: КНЕУ, 2010. – 316 с.

66. Стан і проблеми забезпечення інформаційної безпеки /[Електронний ресурс] – Режим доступу: http://old.niss.gov.ua/book/otch/roz13.htm

67. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко// [Електронний ресурс] – Режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/download/3172

68. Стратегії національної безпеки України», затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015 /[Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015

69. Стратегічне управління суб'єктами господарювання : проблеми теорії та практики. монографія / авт. кол. О. Л. Яременко, Г. В. Строкович та ін.; Нар. укр. акад., [каф. економіки підприємства]. – Хірків : Вид-во НУА, 2013. – 504 с.

70. Судакова, О. І. Стратегічне управління фінансовою безпекою підприємства [Текст] / О . І . Судакова / /Економічний простір. – 2008. – № 9.– С. 140–148.

71. Україна-2020: зовнішньополітичні виклики та можливості наступного десятиріччя. Український інститут публічної політики. [Електронний ресуср] – Режим доступу: http://uipp.org.ua/uploads/news_ message/at_file_uk/0070/38.pdf.

72. Фінансова безпека: суть та місце в системі економічної безпеки держави /[Електронний ресурс] – Режим доступу: http://bookss.co.ua/book_finansova-bezpeka-lekci_845/3_2.1.-finansova-bezpeka-sut-ta-misce-v-sistemi-ekonomichno-bezpeki-derzhavi – Назва з екрану

73. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення [Текст] :монографія / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич, В. В. Каркавчук ; за ред. Т. Г. Васильціва. – Львів : Ліга-Прес, 2012. – 386 с.

74. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46– 56.

75. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2004. – 136 с.

76. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №8. – С.30–33.

77. Черняк Г.М. Оцінювання рівня економічної безпеки енергетичних підприємств в умовах євроінтеграції. /Г.М. Черняк//[Електронний ресурс]/ Економічний вісник Національного технічного університету України «Київський політехнічний інститут». – 2015. – № 12. – С. 159-166. – Режим доступу: http://nbuv.gov.ua/UJRN/evntukpi_2015_12_26

78. Шкарлет С.М. Економічна безпека підприємства: інноваційний аспект: монографія / С.М. Шкарлет. – К.: Книжкове видавництво Національного авіаційного ун-ту, 2007. – 436 с.

79. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. – СПб, 2007. – 138 с.

80. Штангрет А.М. Обліково-аналітичне забезпечення управління економічною безпекою підприємства. [Електронний ресурс] – Режим доступу: http://aphd.ua/publication-31/

81. Экономика предприятия: Учебник / Под общ. ред. д-ра экон. наук, проф. С.Ф. Покропивного. К.: КНЭУ, 2005. - 238 с.

82. Ярочкин В.И. Система безопасности фирмы / В.И. Ярочкин. - 3-е изд., перераб. и доп. - М.: Ось-89, 2003. - 352 с.

Інформаційні ресурси

1. http://rada.gov.ua/ - Офіційний портал Верховної Ради України
2. http://smida.gov.ua – Електронна база підприємств і організацій України
3. http://www.nbuv.gov.ua – Сайт Національної бібліотеки України ім. В.І. Вернадського
4. http://allsecurity.info – Інформаційно-аналітичний портал по безпеці