МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА

К. А. МАМОНОВ, О. В. ПИРКОВА

СТРАТЕГІЧНИЙ ТА ІННОВАЦІЙНИЙ МЕНЕДЖМЕНТ У СФЕРІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

КОНСПЕКТ ЛЕКЦІЙ

(*для студентів денної і заочної форм навчання освітнього рівня «магістр» спеціальності 073 – Менеджмент. Управління фінансово-економічною безпекою*)

Харків
ХНУМГ ім. О. М. Бекетова
2016

Мамонов К. А. Конспект лекцій з дисципліни «Стратегічний та інноваційний менеджмент у сфері фінансово-економічної безпеки» (для студентів денної і заочної форм навчання освітнього рівня «магістр» спеціальності 073 – Менеджмент. Управління фінансово-економічною безпекою) / К. А. Мамонов, О. В. Пиркова ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2016. – 56 с.

Автори: К. А. Мамонов,
О. В. Пиркова

Рецензент: канд. екон. наук, доц. М. В. Кадничанський

Рекомендовано кафедрою фінансово-економічної безпеки, обліку і аудиту, протокол № 1 від 27.08.2013 р.

Схвалено науково-методичною радою факультету Економіки і підприємництва, протокол від «30» серпня 2013 року № 1.

ЗМІСТ

Стор.

ВСТУП

У сучасних умовах господарювання на вітчизняних підприємствах для забезпечення їх розвитку необхідно сфокусувати увагу на формуванні та реалізації фінансово-економічної безпеки. При цьому стратегічні аспекти та інноваційний інструментарій відіграє важливе значення, оскільки створює умови для розвитку у довгостроковій перспективі.

Метою викладання навчальної дисципліни «Стратегічний та інноваційний менеджмент у сфері фінансово-економічної безпеки» є отримання спеціальних знань щодо методології та інструментарію формування й використання теоретико-методичних положень й практичних рекомендацій стратегічного та інноваційного менеджменту у сфері фінансово-економічного безпеки на підприємствах для підготовки фахівців сучасного рівня з урахуванням особливостей стратегічного розвитку суб'єктів господарювання на основі інноваційних пріоритетів.

Основними завданнями вивчення дисципліни «Стратегічний та інноваційний менеджмент у сфері фінансово-економічної безпеки» є:

- набуття та засвоєння знань з теорії стратегічного та інноваційного менеджменту;
- набуття практичних навичок і особистих якостей майбутніх спеціалістів, які потрібні для формування та функціонування фінансово-економічної безпеки в організації.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні підходи до організації аналітичної та управлінської роботи на підприємстві;
- застосування методики і техніки стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки;
- особливості формування стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки на вітчизняних підприємствах у сучасних економічних умовах господарювання;
- інформаційно-аналітичне забезпечення стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки;
- місце та роль стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки.

вміти:

- використовувати інструментарій стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки для прийняття управлінських рішень;
- застосовувати методи, моделі, інструменти стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки;
- впроваджувати моделі й технології стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки на підприємстві;
- застосовувати результати використання моделей та технологій стратегічного й інноваційного менеджменту у сфері фінансово-економічної безпеки для прийняття управлінських рішень;
- на основі відповідних технологій, методів, моделей, будувати ефективно діючий механізм управління підприємством, з урахуванням напрямів здійснення

фінансово-економічної безпеки.

Дисципліна «Стратегічний та інноваційний менеджмент у сфері фінансово-економічної безпеки» складається із трьох змістових модулів та 9 тем, у яких розглянуто теоретичні підходи щодо визначення стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки. Технології визначення стратегії економічної безпеки підприємства, установи, організації, види стандартів безпеки, розробка й впровадження стратегій безпеки, видів та напрямів діяльності підприємства, установи, організації, формування й використання моделей безпеки, напрями розробки й впровадження перспективних планів фінансово-економічної безпеки в сфері стратегічного та інноваційного менеджменту.

Змістовий модуль 1
Теоретичний базис і технології стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки

Лекція 1

Тема 1. Теоретичні підходи щодо визначення стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки

1.1. Визначення поняття «стратегія» в системі стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки.
1.2. Напрями розробки й впровадження стратегії фінансово-економічної безпеки на підприємстві.
1.3. Стратегічне управління для забезпечення фінансово-економічної безпеки на підприємстві.
1.4. Інноваційний менеджмент в сфері фінансово-економічної безпеки підприємства.

Література: [13, 14, 16, 17, 20, 22, 23, 24, 25, 34, 35, 38, 53, 57, 58, 61, 62, 63, 64, 72, 73].

1.1. Визначення поняття «стратегія» в системі стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки

У сфері фінансово-економічної безпеки підприємства для забезпечення його розвитку важливого значення має формування стратегії, обґрунтування теоретико-методичних положень щодо її визначення.

Формування стратегії – це одна з функцій управління, що являє собою процес вибору цілей організації і шляхів їх досягнення і впливає на результативність реалізації стратегічного та інноваційного менеджменту у сфері фінансово-економічної безпеки.

Розвиток категорії «стратегія» в аспекті вирішення економічних і

управлінських питань здійснювалось на основі фундаментальних засад, використаних із теорії й практики проведення військових дій.

У контексті сучасного розуміння стратегії, як важливого компонента управління підприємства, важливого значення мають роботи І. Ансоффа, М. Портера, А. Чандлера, П. Друкера, П. Дойля, Г. Мінцберга та ін.

У результаті узагальнення існуючих теоретико-методичних підходів запропоновано визначати стратегію як систему взаємопов'язаних дій, що впливає на формування організаційної структури підприємства, динамічно змінюється в умовах ринкових трансформацій для впровадження інновацій й удосконалення виробничо-господарської структури з метою забезпечення стратегічних переваг у майбутньому і фінансово-економічної безпеки.

1.2. Напрями розробки й впровадження стратегії фінансово-економічної безпеки на підприємстві

При розробці й впровадженні стратегії фінансово-економічної безпеки на підприємств вирішується комплекс питань:

1. Де зараз знаходимося? В рамках цього питання здійснюється: оцінка минулих стратегій, факторів ефективності; аналіз конкуренції та ринків; визначення критичних факторів успіху; визначення стратегічних ресурсів і можливостей.

2. Де ми хочемо бути? При цьому формується місія, бачення, мета, визначаються стратегічні альтернативи та їх ранжування, здійснюється вибір пріоритетних напрямів й визначаються стратегічні переваги.

3. Що нам мішає? Визначаються неефективні команди та вплив на діяльність менеджменту компанії, рівень та спротив змінам, характеризується лідерство та фокус на основі аспектів діяльності та розвитку підприємства.

4. Що ми повинні роботи? Вирішення цього питання лежить в площині таких питань: проектне впровадження стратегії; програма роботи керівництва в стратегічному напрямі; систематичне планування; зв'язок стратегічних успіхів з винагородою, трансформація стратегії в структуру, управлінський облік, бюджетування.

Конкретизуючи стратегічні питання визначимо наступні:

- ✓ якими напрямами діяльності займається компанія (визначення границь бізнесу або бізнес-сегментів компанії);
- ✓ який із сегментів приносить найбільший прибуток (має найбільшу рентабельність);
- ✓ які конкурентні позиції компанії у визначених сегментах (наскільки вона краща з точки зору її конкурентних переваг): відносна доля ринку компанії у визначеному сегменті; тенденції змін відносної питомої ваги ринку; можливі річні темпи зростання цього сегменту ринку; показники прибутку на використаний капітал для кожного сегменту;
- ✓ які конкурентні переваги, що лежать в основі успіху компанії у визначених сегментах ринку;
- ✓ наскільки успішною є галузь, в якій працює компанія;

- ✓ яка репутація покупців про діяльність компанії на представленому сегменті ринку (споживчі критерії вибору постачальника у представленому сегменті ринку);
- ✓ яка діяльність конкурентів в цьому сегменті ринку;
- ✓ як збільшити прибутковість компанії у визначеному сегменті у короткостроковому періоду;
- ✓ як збільшити прибутковість компанії у представленому сегменті у довгостроковому періоді діяльності.

Для формування стратегії на підприємстві здійснюють наступні етапи:

- ➢ визначення напрямів стратегії;
- ➢ імплементація (впровадження) стратегії;
- ➢ реалізація стратегії.

На першому етапі – визначення напрямів стратегії – характеризується напрямам розвитку і представляє собою комплексний план розвитку або модель дій суб'єктів підприємницької діяльності, що ґрунтується на історичних аспектах й функціональних особливостях, в яких функціонує підприємство. При цьому необхідно визначати «свою унікальність» на основі вміння, досвіду і талантів, враховуючи можливості майбутнього розвитку компаній;

2 етап – імплементація (впровадження) стратегії у вигляді комплексу ресурсозабезпечених дій, «принципів поведінки», які спрямовані на досягнення поставлених на першому етапі цілей та враховуючи особливості діяльності компанії;

3 етап – реалізація стратегії як системи перманентно трансформуючих організаційних дій і управлінських підходів щодо реалізації розроблених стратегічних напрямів.

1.3. Стратегічне управління для забезпечення фінансово-економічної безпеки на підприємстві

Суть стратегічного управління полягає в тому, що в організації, з одного боку, існує чітко організоване комплексне стратегічне планування, з іншого боку – структура управління фірмою адекватна «формальному» стратегічному плануванню і побудована так, щоб забезпечити розробку довгострокової стратегії для досягнення цілей фірми і створення управлінських механізмів реалізації цієї стратегії через систему планів.

Узагальнюючи існуючи теоретико-методичні підходи щодо визначення стратегічного менеджменту у сфері фінансово-економічної безпеки запропоновано наступне визначення: ***стратегічний менеджмент*** – це процес формулювання місії і цілей організації, вибору специфічних стратегій для визначення й одержання необхідних ресурсів і їхнього розподілу з метою забезпечення ефективної роботи організації в майбутньому шляхом побудови системи фінансово-економічної безпеки.

Принципами стратегічного менеджменту в сфері фінансово-економічної безпеки є:

1. Відкритість.

2. Комплексний підхід.
3. Орієнтація на майбутнє.
4. Творчій підхід.
5. Орієнтація на результати.
6. Спільна діяльність.
7. Забезпечення перманентної безпеки на кожному етапі виробничо-господарської діяльності.

Управлінський цикл стратегічного менеджменту складається із наступних елементів: збір і аналіз інформації, розробка стратегії, програмування стратегії, реалізація стратегії, моніторинг і контроль.

1.4. Інноваційний менеджмент в сфері фінансово-економічної безпеки підприємства

Узагальнюючи теоретико-методологічні підходи до визначення інноваційного менеджменту в сфері фінансово-економічної безпеки запропоновано наступне поняття ***інноваційний менеджмент*** як система являє собою комплекс формальних і неформальний правил, принципів, норм, установок і ціннісних орієнтацій, що регулюють різні сфери інноваційної діяльності і забезпечують формування й використання системи фінансово-економічної безпеки на підприємстві.

До функцій інноваційного менеджменту в сфері фінансово-економічної безпеки відносяться: прогнозування, планування, аналіз зовнішнього середовища, аналіз внутрішнього середовища, види рішень, мотивація, контроль, впровадження інновацій в систему фінансово-економічної безпеки підприємства, які мають стратегічну й функціональну (оперативну) орієнтованість.

Питання для розгляду:

1. Визначте поняття стратегії.
2. Назвіть етапи розробки стратегії на підприємствах, установах, організаціях.
3. Визначте види стратегій.
4. Охарактеризуйте стратегічний менеджмент та його впровадження на підприємствах, організаціях, установах.
5. Визначте інноваційний менеджмент в сфері фінансово-економічної безпеки.

Тема 2. Технології визначення стратегії фінансово-економічної безпеки підприємства, установи, організації

2.1. Інформаційне забезпечення стратегії фінансово-економічної безпеки підприємства, установи, організації.
2.2. Характеристика систем інформаційного захисту.
2.3. Технології розробки й впровадження стратегії фінансово-економічної безпеки підприємства, установи, організації.

Література: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 17, 20, 21, 22, 23, 30, 33, 35, 38, 43, 51, 53, 57, 58, 61, 62, 63, 64, 70, 71, 84, 86].

2.1. Інформаційне забезпечення стратегії фінансово-економічної безпеки підприємства, установи, організації.

У рамках стратегії економічної безпеки підприємства, установи, організації об'єктами захисту з урахуванням їх пріоритетів є:

1) особа;

2) інформація;

3) матеріальні цінності.

Ринкові відносини з їх невід'ємною частиною – конкуренцією обов'язково вимагають протидії зовнішнім і внутрішнім впливам.

Для розробки й впровадження стратегії економічної безпеки підприємства, установи, організації важливе значення має інформація, яка характеризується як результат відображення та обробки в людській свідомості різноманіття навколишнього світу, відомостей про предмети, що оточують людину, явища природи, діяльність інших людей і т. п.

Відповідно до Закону України «Про інформацію» визначають такі її види:

- ✓ статистична інформація;
- ✓ масова інформація;
- ✓ інформація про діяльність державних органів влади й органів місцевого і регіонального самоврядування;
- ✓ правова інформація;
- ✓ інформація про особу;
- ✓ інформація довідково-енциклопедичного характеру;
- ✓ соціологічна інформація.

Інформацію також можна підрозділити на:

1) життєво важлива незамінна інформація, наявність якої необхідна для функціонування системи;

2) важлива інформація – інформація, що може бути замінена чи відновлена, але процес її відновлення важкий і пов'язаний з великими витратами;

3) корисна інформація – інформація, яку важко відновити, однак система може досить ефективно функціонувати і без неї;

4) несуттєва інформація – інформація, без якої система продовжує існувати.

Для оцінки інформації використовуються наступні показники:

- *важливість*;
- *повнота*;
- *адекватність*;
- *релевантність*;
- *толерантність*.

2.2. Характеристика систем інформаційного захисту

Для забезпечення захисту зовнішніх і внутрішніх потоків у рамках стратегії фінансово-економічної безпеки застосовуються технології, які представлені у таблиці 2.1.

Таблиця 2.1 – Системи інформаційного захисту

Назва системи інформаційного захисту	Характеристика
1	**2**
Системи електронного захисту	комп'ютерна безпека (маркування файлів; формування особистих паролів; шифрування інформації; забезпечення захисту приміщень, де знаходяться інформаційні системи; централізоване управління інформацією; побудова систем додаткової перевірки інформації з можливим її блокуванням); технологічна безпека (застосування сучасних технологічних систем і засобів, що попереджають і блокують відтік інформації).
Системи персонального захисту	відкриті системи, коли персональний користувач має доступ до інформації; ізоляційні системи, в яких користувач забезпечує блокування деякої інформації відповідно до інших груп користувачів; управляючі системи, інформація в яких не може формуватись або використовуватись без дозволу користувача; закриті системи, в яких інформацію запрограмовано керівниками підрозділів або підприємств й без їх дозволу не можливо її отримати.
Системи психологічного захисту	орієнтовані на відповідність психологічного, морального й розумового рівня користувача автоматизованим системам управління для мінімізації помилок у системі й витоку інформації.
Віртуальні системи захисту	спрямовані на об'єднання в єдиний комплекс всіх суб'єктів, зацікавлених у формуванні й отриманні інформації із інформаційними технологіями, в яких захист відбувається системою самостійно через відповідний інструментарій.
Орієнтовані системи захисту	системи, що орієнтуються на список – полягають у використанні охороною ідентифікаційного списку зареєстрованих користувачів, у яких знаходиться спеціальний ключ і без дозволу охорони не можливо ввійти в інформаційну систему підприємства; системи, що орієнтуються на ключ – пов'язані з використанням відповідного ключа користувачем інформації, описання якого знаходиться у охорони; системи, що орієнтуються на керівника: в них вхід в систему, формування

Продовження таблиці 2.1

1	2
	й використання інформації не можливий без електронного дозволу керівника. За своїми функціональними особливостями ця система подібна закритій системі персонального захисту. Натомість, якщо в останній можливі варіанти (підпорядкування керівникам підрозділів та інших структурних елементів підприємства), то в системі, що орієнтується на керівника, вхід можливий тільки за згодою керівника підприємства. Перевагою цієї системи є залучення до захисту кваліфікованих спеціалістів, які контролюють не тільки процес формування й використання інформації на підприємстві, але й контролюють самих користувачів. Недоліком поданої системи є залучення в процес захисту інформації третіх осіб, які можуть впливати на її формування й використання. Важливе значення має професійні, моральні, психологічні й етичні якості цих осіб. Розглядаючи систему, орієнтовану на керівника, то слід зазначити можливі ускладнення щодо доступності до інформації у випадку відсутності керівника; комбіновані системи, які узагальнюють в собі ознаки й особливості систем, що представлено вище. Перевагою цієї системи захисту є те, що її можна побудувати самостійно, базуючись на відповідних системах і вона має ознаки до самоаналізу й саморозвитку. Проте, в рамках комбінованих систем можливі недоліки, які пов’язані із іншими системами інформаційного захисту.

2.3. Технології розробки й впровадження стратегії фінансово-економічної безпеки підприємства, установи, організації

Для розробки й впровадження стратегії економічної безпеки підприємств використовуються наступні показники та технології:

1. *Збалансована система показників* (*BalancedScorecard – BSC*).
2. *Система показників відповідальності* (*ASC*).
3. *Модель ділової переваги* (*BEM*).
4. *Піраміда результативності МакНейра*.
5. *Бенчмаркінг*.
6. *SWOT-аналіз*.
7. *Дискрімінантний аналіз*.
8. *Кластерний аналіз*.
9. *Матриця Бостонської консалтингової групи* (*BCG*) *«Зростання/Частка»*.
10. *Модель GE/McKinsey*.
11. *Матриця спрямованої політики* (*модель Shell/DPM*).

У рамках розробки стратегії фінансово-економічної безпеки використовується інструментарій, який представлено на рисунку 2.1.

Рисунок 2.1 – Інструментарій фінансово-економічної безпеки, який використовується в рамках розробки й впровадження стратегії економічної безпеки на підприємства, організаціях, установах

Питання для розгляду:

1. Охарактеризуйте напрями інформаційного забезпечення стратегії фінансово-економічної безпеки на підприємстві, організації, установі.
2. Визначте системи інформаційного захисту.
3. Охарактеризуйте технології розробки й впровадження стратегії фінансово-економічної безпеки підприємства, установи, організації.
4. Визначте інструментарій фінансово-економічної безпеки, який використовується в рамках розробки й впровадження стратегії економічної безпеки на підприємства, організаціях, установах.

Змістовий модуль 2
Види стандартів безпеки, розробка й впровадження стратегій безпеки, видів та напрямів діяльності підприємства, установи, організації, формування й використання моделей безпеки

Лекція 2

Тема 3. Штатний розклад підприємства, установи, організації. Стандарти безпеки діяльності установи, організації, підприємства. Стандарти безпеки підприємства, установи, організації. Стандарти безпеки інформаційних технологій установи, організації, підприємства. Стандарти безпеки документування і документообігу в установі, організації, підприємстві. Стратегія безпеки діяльності та розвитку установи, організації, підприємства

3.1. Штатний розклад підприємства, установи, організації.
3.2. Стандарти безпеки діяльності установи, організації, підприємства. Стандарти безпеки інформаційних технологій установи, організації, підприємства. Стандарти безпеки документування і документообігу в установі, організації, підприємстві.
3.3. Стратегія безпеки діяльності та розвитку установи, організації, підприємства.

Література: [25, 57, 65, 67, 82, 83].

3.1. Штатний розклад підприємства, установи, організації

Штатний розклад підприємства, установи, організації слугує підставою при прийнятті рішень власником підприємства стосовно кадрових питань, зокрема щодо прийняття громадян на роботу, визначення посадового окладу, тарифної ставки працівника.

Штатний розклад є внутрішнім (локальним) нормативно-правовим документом підприємства, установи, організації (далі – підприємство), який у зведеному вигляді:

- фіксує розподіл праці між працівниками;
- закріплює структурний та чисельний склад працівників і місячний фонд заробітної плати;
- конкретизує перелік посад і професій;
- встановлює розмір основної заробітної плати щодо конкретної посади, професії, а також розмір надбавок (доплат), якщо це передбачено положенням про оплату праці.

Саме на підставі штатного розкладу, як і Правил внутрішнього трудового розпорядку та посадових (робочих) інструкцій, власник або уповноважений ним орган приймає рішення з кадрових питань, зокрема щодо прийняття громадян на роботу, переведення працівників на іншу роботу, визначення посадового

окладу, тарифної ставки (окладу) конкретного працівника відповідно до його посади (кваліфікації). А кадрова служба – здійснює добір персоналу, оформляє відповідні кадрові документи, у т. ч. накази про прийняття на роботу, переведення на іншу роботу, встановлення надбавок (доплат), аналізує якісний склад працівників і вносить пропозиції щодо його поліпшення, в установленому порядку готує облікову та інформаційно-довідкову документацію, відповідну статистичну звітність.

Відповідно до ч. 3 ст. 64 Господарського кодексу України штатний розклад на підприємстві, установі, організації розробляється самостійно (зараз порядок і норми щодо складання штатного розпису законодавчо не врегульовано; їх прийнято лише для бюджетних установ та організацій). Таким чином, під час складання штатного розкладу можна використовувати рекомендації, подані в цій статті (базуються вони на досвіді і практиці великих і малих підприємств різних форм власності), і роз'яснення, вміщені в листі Міністерства праці та соціальної політики України від 20 січня 2005 року № 18-23. Розроблення штатного розкладу має здійснюватися на основі затверджених структури підприємства і чисельності його працівників, положення про оплату праці (як правило, є додатком до колективного договору) та з урахуванням вимог нормативно-правових актів, зокрема, Закону України «Про оплату праці» від 24 березня 1995 року № 108/95-ВР, Інструкції про порядок ведення трудових книжок працівників, затвердженої наказом Міністерства праці України, Міністерства юстиції України, Міністерства соціального захисту населення України від 29 липня 1993 року № 58, Національного класифікатора України «Класифікатор професій» ДК 003:2005 (далі – КП), випусків Довідника кваліфікаційних характеристик професій працівників. Розробляє штатний розклад, як правило, **відділ організації праці та заробітної плати**. На підприємствах, організаціях, установах де такого відділу не створено, розроблення цього локального нормативного акта може покладатися на інший структурний підрозділ (наприклад, кадрову службу) або, за рішенням керівника підприємства, на окремого спеціаліста в порядку, передбаченому внутрішніми нормативними актами.

Штатний розклад складається у довільній формі.

3.2. Стандарти безпеки діяльності установи, організації, підприємства. Стандарти безпеки інформаційних технологій установи, організації, підприємства. Стандарти безпеки документування і документообігу в установі, організації, підприємстві

Стандарти безпеки підприємства, установи, організації складаються із:

- концепції корпоративної безпеки підприємств;
- освітнього стандарту зі спеціальності 8.18010014 «Управління фінансово-економічною безпекою»;
- законопроектів «Про охоронну діяльність в Україні», «Про детективну діяльність», «Про служби безпеки суб'єктів господарювання та інших юридичних осіб», «Про комерційну таємницю в Україні»;
- Державного стандарту України «Захист інформації. Технічний захист інформації.

Порядок проведення робіт». ДСТУ 3396.1-96.

Для забезпечення реалізації стандартів безпеки на підприємстві, організації, установі необхідно забезпечити ефективність діловодства та документального забезпечення. Термін «діловодство» визначається наступним чином: галузь діяльності, що забезпечує документування і організацію роботи з офіційними документами. Поряд з терміном «Діловодство» в останні роки вживається і синонімічні йому термін «Документаційне забезпечення управління». Виникнення його пов'язане зі зміною організаційно-технічної основи діловодства та методологічних підходів до його вдосконалення, що стало можливим завдяки активному впровадженню в сферу роботи з документами коштів обчислювальної техніки і сучасних інформаційних технологій створення, збору, обробки, накопичення, зберігання, пошуку і використання інформації в управлінні. Таким чином, термін «документаційне забезпечення управління» як би підкреслює інформаційно-технологічну складову в сучасній організації діловодства.

Рух документів на підприємстві, організації, установі з моменту їх створення або одержання до завершення виконання або відправлення називається документообігом. Від чіткості й оперативності обробки та утворення документа залежить швидкість отримання інформації, необхідної для вироблення рішення. Тому раціональної організації документообігу завжди приділяється велика увага. Вся документація установи поділяється на три документопотока:

- вхідні (надходять) документи;
- вихідні (відправляються) документи;
- внутрішні документи.

Кожен з документопотоків має свою особливість в складі, кількості, обробці та рух. Кількість документів всіх потоків за рік складе обсяг документообігу установи. Величина документообігу потрібна для розрахунку необхідної чисельності діловодного персоналу, розрахунку ефективності застосування засобів механізації та автоматизації діловодства. В цілому вона показує завантаженість всього управлінського апарату, тому що всім його працівникам доводиться мати справу з документами. У технологічному ланцюжку обробки і руху документів можна виділити етапи: прийом первинна обробка документів; попередній розгляд і розподіл документів; реєстрація; контроль за виконанням; інформаційно-довідкова робота; виконання документів і відправлення.

Створення документів або документування може здійснюватися надприродною мовою або на штучних мовах з нових носіїв інформації. При документуванні природною мовою створюються текстові документи – документи, що містять мовну інформацію, зафіксовану будь-яким типом письма або будь-якою системою звукозапису. Текстовий документ, створений за допомогою листа, – це традиційний документ на паперовому носії чи відеограми документа – зображення документа на екрані електронно-променевої трубки. Юридична сила документа забезпечується встановленим для кожного різновиду документу комплексом реквізитів-обов'язкових елементів оформлення документа (назва автора документа, адресата, підпис, дата, номер документа, гриф затвердження, друк та ін.). Сучасні вимоги до оформлення організаційно-розпорядчого (адміністративної) документації зафіксовані в державному стандарті (ГОСТ Р б.30-97 «Уніфіковані системи

документації. Система організаційно-розпорядчої документації. Вимоги до оформлення документів»).

Державним стандартом встановлений не тільки склад реквізитів (всього їх 29), але і зони і послідовність і розміщення на документі. Сукупність реквізитів документа і схема їх розташування на документі складають формуляр документа. Формуляр також регламентований державним стандартом, тому для правильного складання документа необхідно знати не тільки реквізити документа, але і схему (модель) їх розташування на документі. Наявність формуляра, встановленого державним стандартом, забезпечує єдність документування і єдність документації, як в рамках однієї установи, так і в цілому в країні.

У суспільстві документи є основними носіями управлінської, наукової, технічної, статистичної та іншої соціально значущої інформації. Документи – носії первинної інформації, саме в документах інформація фіксується вперше. Це властивість і дозволяє відрізняти документи від інших джерел інформації – книг, газет, журналів та ін., що містять перероблену, вторинну інформацію. Фіксація, відображення інформації в документі забезпечує її збереження і накопичення, можливість передачі в часі і просторі, можливість звертатися до інформації через багато часу після її створення. У соціальному плані будь-який офіційний документ поліфункціонален, тобто одночасно виконує кілька функцій, що дозволяє йому задовольняти різні людські потреби. Серед функцій документа виділяються загальні і спеціальні. До загальних функцій документа відносяться: інформаційна: будь-який документ створюється для збереження інформації, бо на необхідності зафіксувати інформацію-причина появи будь-якого документа; соціальна: документ є соціально значущим об’єктом, оскільки будь-який документ породжений тієї чи іншою соціальною потребою; комунікативна: документ виступає як засіб зв’язку між окремими елементами суспільної структури, зокрема між установами, культурна: документ – засіб закріплення та передачі культурних наприклад в науково-технічній документації знаходить відображення рівень наукового та технічного розвитку суспільства.

До специфічних функцій документа відносяться: управлінська: документ є інструментом управління, цієї функцією наділені так звані управлінські документи (планові документи, звітні, організаційно-розпорядчі та ін.), спеціально створюються для реалізації цілей управління; правова: документ є засобом закріплення і зміни правових норм і правовідносин у суспільстві; цією функцією наділені законодавчі та нормативні правові акти, спочатку створюються для фіксації правових норм і правовідносин, а також документи, які набувають правову функцію на час (наприклад, для використання в якості судового докази це може бути будь-який документ); функція історичного джерела: документ виступає як джерела історичних зведень про розвиток суспільства; цю функцію набуває тільки частина що створюються в суспільстві документів (приблизно 12-14 %) і тільки після того, як документи виконають свої оперативні функції і надійдуть на зберігання. Будь-який документ, що створюється в суспільстві, є елементом системи більш високого рівня, він входить у відповідну систему документації в якості її елемента. Під системою документації розуміється сукупність документів, взаємопов’язаних за ознаками походження, призначення, виду, сфери діяльності, єдиних вимог до

їх оформлення. До теперішнього часу в документознавства не існує несуперечливої наукової класифікації систем документації, видів і різновидів документів.

Лекція 3

Офіційні документи в залежності від обслуговування ними сфери людської діяльності підрозділяються на управлінські, наукові, технічні (конструкторські), технологічні, виробничі та ін. Управлінські документи становлять ядро засновницької документації. Саме вони забезпечують керованість об'єктів як в рамках всієї держави, так і в окремій організації. Управлінські документи і складають власне об'єкт діловодства. Ці документи представлені комплексом систем, основними з яких є такі системи документації: організаційно-правова документація, планова документація; розпорядча документація; інформаційно-довідкова й довідково-аналітична документація, звітна документація; документація щодо забезпечення кадрами (по особовому складу); фінансова документація (бухгалтерський облік і звітність); документація з матеріально-технічного забезпечення; договірна документація, документація з документаційного та інформаційного забезпечення діяльності установи та інші системи документації, включаючи і ті, які відображають основну діяльність установи, організації або підприємства, наприклад на виробничому підприємстві – це виробнича документація, в лікувальній установі – система медичної документації, у виші – система документації з вищої освіти і т. д.

Забезпечення документування – це лише одна складова діловодства, друга його складова – це організація роботи з документами. Організація роботи з документами припускає організацію документообігу установи. Документообіг установи – це сукупність взаємопов'язаних процедур, що забезпечують рух документів в установі з моменту їх створення або надходження і до завершення виконання або відправлення. З метою раціональної організації документообігу всі документи розподіляються по документопотоках, наприклад, реєструються і не реєструються документи; вхідні, вихідні і внутрішні документи; документи, що направляються і надходять в вищестоящих організаціях, або документи, що направляються в або надходять з підвідомчих організацій, і т. д. Під документопотоків розуміється сукупність документів, що виконують певне цільове призначення в процесі документообігу.

Характеристикою документообігу є його обсяг. Під об'ємом документообігу розуміється кількість документів, що надійшли в організацію та створених нею протягом певного періоду часу, як правило року. Обсяг документообігу – важливий показник, який використовується як критерій при вирішенні питань вибору організаційної форми діловодства, організації інформаційно-пошукової системи по документах установи, структури служби діловодства, її штатного складу та інших обліку документів. Облік документів забезпечується їх реєстрацією – записом облікових даних про документ за встановленою форі, що фіксує факт створення документа, його відправлення чи одержання. Поряд з функцією обліку документів реєстрація дозволяє здійснювати контроль виконання документів, вести пошук

документів на запити підрозділів і працівників установи.

Нормативно-методична база діловодства – це сукупність законів, нормативних правових актів та методичних документів, регламентують технологію створення, обробки, зберігання та використання документів в поточній діяльності установи, а також регламентують роботу служби діловодства – її структуру, функції, штати, технічне забезпечення та деякі інші аспекти.

3.3. Стратегія безпеки діяльності та розвитку установи, організації, підприємства

Стратегія економічної безпеки передбачає визначення мети і завдань системи гарантування економічної безпеки, напрямів їх розв'язання, а також форм і методів застосування відповідних сил і засобів, можливість їхнього перегрупування, створення резервів для нейтралізації та локалізації можливих загроз.

Тактика економічної безпеки – це більш динамічна частина політики економічної безпеки, яка змінюється залежно від дії внутрішніх і зовнішніх загроз, зміни пріоритетності національних економічних інтересів тощо. Складність та мінливість економічної та соціальної ситуації потребує застосування різноманітних тактичних заходів щодо гарантування економічної безпеки.

Важливо чітко окреслити стратегічні цілі й не плутати їх з тактичними заходами, інколи вимушеними, але потрібними задля досягнення певної стратегічної мети. Отже, визначення стратегії і тактики сприятиме повноцінному функціонуванню системи гарантування економічної безпеки, здійсненню ефективної політики економічної безпеки.

У Конституції України чітко зазначено, що разом із захистом суверенітету і територіальної цілісності України гарантування її економічної безпеки є найважливішою функцією держави, справою всього українського народу. Економічній безпеці притаманний інтегративний характер, оскільки вона є результатом спільних зусиль усієї нації, що виявляється через дії всіх гілок влади (від всеукраїнського рівня до місцевого), наявних у державі сил і засобів, об'єднань громадян та окремих осіб.

Розробляючи стратегію, слід ураховувати глобальні тенденції переходу до постіндустріального напрямку розвитку та формування так званого інформаційного суспільства. Ігнорування цих тенденцій, зумовлених технологічним прогресом та інформаційною революцією, небезпечне тим, що Україна може стати жертвою інформаційно-технологічного колоніалізму, який набагато більше загрожує державності, а ніж сировинний колоніалізм.

Стратегія економічної безпеки України має, зокрема, містити:

- засадничі положення формування та підтримки функціонування системи гарантування економічної безпеки України;
- характеристику внутрішніх і зовнішніх загроз економічній безпеці та моніторинг факторів, що підривають стійкість соціально-економічної систем и держави;
- критерії та індикатори економічної безпеки;
- характеристику національних економічних інтересів;

• заходи та механізми державної політики щодо гарантування економічної безпеки на національному, регіональному і глобальному рівнях.

Державна економічна стратегія й загалом національна безпека мають ґрунтуватися на ідеології розвитку (системі наукових поглядів, що включає не тільки економіку, а й філософію, соціологію, інформатику, право, політологію, геополітику тощо), що враховує стратегічні пріоритети і національні інтереси, унаслідок чого загрози безпеці мінімізуються. Якщо ринкові сили не можуть самі вивести країну на орбіту розвитку, то потрібно на базі глибокого аналізу ринкової ситуації закласти підвалини підйому виробництва. Отже, без ідеології розвитку, без культивування промислового і науково-технічного піднесення не можна гарантувати економічну безпеку.

Відновлення економічного зростання потребує відновлення платоспроможного попиту й у споживчому секторі, і в інвестиційному. Відомо, що низький платоспроможний попит призводить до зникнення багатьох видів виробництв. А надмірний платоспроможний попит, особливо за зниження виробництва і, відповідно, пропонування товарів і послуг, спричинює зростання цін, створює «навантаження» на емісію грошей і посилює інфляцію.

Розширення сукупного попиту потребує активізації інвестиційної політики, у чому важливу роль відіграє держава. Вона має формувати стабільні умови господарювання, створюючи імпульси щодо інвестування прибутку й амортизаційних відрахувань у відновлення інтелектуально-кадрового, техніко-технологічного, виробничого потенціалу.

Один з напрямків економічної стратегії держави у сфері гарантування безпеки полягає у створенні системи гнучкого регулювання ринкової економіки. Зрозуміло, саме по собі регулювання не гарантує безпеки. Воно може бути не тільки корисним, а й шкідливим, якщо намагатися відновити форми регулювання, що не виправдали себе. Насамперед не можна забувати, що йдеться про регулювання не просто економіки, а ринкової її моделі. Важливо не тільки не порушити механізми саморегуляції, а й забезпечити умови для як найдійовішої роботи цих механізмів. Для цього суб'єкти ринку мають послуговуватися досить повною інформацією про розвиток економіки в цілому, завдання структурної політики, пріоритети державної підтримки, так звані провали ринку; прогнозовані макроекономічні показники та ін. Звичайно, настільки складне завдання виконують не тільки державні керівні структури, а й суспільні та приватні аналітичні центри. Загалом роль держави полягає в пізнанні причинно-наслідкових та інших залежностей у ринковій економіці, у попередженні тих стихійних моментів розвитку, що загрожують національній безпеці, у з'ясуванні сфер, здатних принести в перспективі найбільший прибуток.

Сутність і стратегія економічної безпеки не вичерпуються проблемами відновлення економічного зростання на підставі нової структурної політики, задоволення споживчого й інвестиційного попиту, розвитку ринку цінних паперів, створення конкурентного середовища, оптимізації відносин власності й менеджменту, створення гнучкої системи державного регулювання ринкового типу. Стратегія не стане дійовим інструментом політики, якщо не буде конкретизовано завдання безпеки в окремих сферах економіки: у галузях

матеріального виробництва; у науково-технічній, соціальній і зовнішньоекономічній сферах; у регіонах.

Державна стратегія у сфері гарантування економічної безпеки України має орієнтуватися насамперед на підтримку достатнього рівня виробничого, науково-технічного потенціалу, на недопущення зниження рівня життя населення до межових значень, що може викликати соціальну напруженість, на запобігання конфліктів між окремими верствами і групами населення, різними націями й народностями. Ця стратегія має втілюватись у життя передовсім завдяки системі безпеки, котру утворюють органи законодавчої, виконавчої і судової влади, суспільні й інші організації та спілки.

На мікроекономічному рівні в ході здійснення структурної політики на перший план виходять завдання підтримки й стимулювання розвитку економічно ефективних підприємств і організацій, ліквідації чи реорганізації недійових економічних структур, упровадження ринкових норм поведінки економічних суб'єктів.

У процесі цієї роботи треба:

• установити «точки зростання», тобто підприємства й організації, які реалізують проекти і програми, що забезпечують, пошук і освоєння реального платоспроможного попиту на вільному ринку;

• визначити роль і місце діючих підприємств у господарській системі, організувати процес ліквідації неефективних підприємств, підвищити дієвість керування державними підприємствами;

• скласти перелік підприємств, продукція яких забезпечить державні потреби;

• установити такі суб'єкти господарювання, в яких контрольний пакет акцій чи «золота акція» мають бути закріплені за державою для впливу на рішення, що їх приймають дані суб'єкти, з метою гарантування економічної безпеки;

• визначити перелік конкретних підприємств, які потребують державної підтримки, для гарантування економічної безпеки.

Неодмінною умовою додержання вимог економічної безпеки є реалізація системи проектів і програм перспективного характеру – як наукових та інноваційних, так і виробничих та інвестиційних.

Стратегія безпеки діяльності та розвитку установи, організації, підприємства потребує вирішення наступних важливих питань:

- формування інформаційно-аналітичного забезпечення процесу створення та реалізації фінансово-економічної безпеки на підприємстві, установі, організації;
- визначення проблемних аспектів та точок зміцнення фінансово-економічної безпеки;
- характеристика інструментів фінансово-економічної безпеки;
- визначення джерел для фінансування заходів фінансово-економічної безпеки;
- забезпечення моніторингу і контролю щодо забезпечення фінансово-економічної безпеки.

Питання для розгляду:

1. Охарактеризуйте стратегію фінансово-економічної безпеки підприємства,

установи, організації.
2. Визначте напрями розробки стратегії фінансово-економічної безпеки.
3. Особливості реалізації стратегії фінансово-економічної безпеки на підприємстві, установі, організації.
4. Охарактеризуйте стандарти фінансово-економічної безпеки.

Лекція 4

Тема 4. Види та напрями діяльності щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства. Види і напрями діяльності установи, організації, підприємства. Моделі економічної безпеки підприємства, установи, організації

4.1. Види та напрями діяльності щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства.
4.2. Види і напрями діяльності установи, організації, підприємства.
4.3. Моделі економічної безпеки підприємства, установи, організації.

Література: [17, 18, 19, 23, 26, 27, 28, 29, 31, 41, 42, 52, 56].

4.1. Види та напрями діяльності щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства

Середовище, в якому працює підприємство, потребує постійної роботи управлінського персоналу над удосконаленням рішень щодо забезпечення його економічної безпеки. Одним із напрямів цього процесу є організація системи безпеки на підприємстві. У зв'язку з цим усі підприємства створюють власні або використовують міжвідомчі служби безпеки.

Міжоб'єктні служби безпеки, як правило, спеціалізуються або на чисто режимно-охоронних послугах (охорона будівель, споруд, транспорту, окремих працівників підприємств, установ, членів їх сімей тощо), або на суто економічних, правових чи консультаційних. Клієнтами таких служб є сукупність малих та середніх підприємств, організацій та установ, для яких важко утримувати власні служби безпеки. Більш великі підприємства, банківські чи інші установи кредитно-фінансової системи також звертаються з окремих питань у ці служби безпеки.

Такі суб'єкти економіки не зможуть забезпечити ефективного функціонування своєї організації без комплексного підходу до питань безпеки. Тому, як правило, вони створюють власні служби безпеки. Структура цих підрозділів залежить від рівня становлення підприємства, масиву питань, вирішення яких покладає на ці служби керівництво організації на тому чи іншому етапі її розвитку. Але в структурі типових служб безпеки повинні обов'язково бути підрозділи, до функцій яких входять такі елементи системи безпеки, як:

- розвідка, контррозвідка з економічних та інших питань;
- внутрішня безпека, режим діловодства, моніторинг факторів ризику;

- режим проходу на об’єкт та охорону його будівель, територій і споруд;
- фізична безпека персоналу;
- протипожежна безпека;
- технічна безпека, до якої входять:
- робота охоронно-технічного обладнання;
- захист засобів зв’язку, комп’ютерних систем та інших комунікаційних мереж;
- радіаційно-хімічна безпека, цивільна оборона;
- безпека перевезень;
- інформаційно-аналітична робота;
- психолого-соціологічна робота;
- рекламно-пропагандистське забезпечення діяльності суб’єкта підприємництва;
- експертна перевірка механізму системи безпеки.

Для ефективного виконання перерахованих функцій важливо врахувати такі допоміжні елементи системи безпеки, як:

а) система повідомлення про екстрений збір;

б) типове планування дій особового складу служби безпеки (далі – СБ), персоналу організації в критичних ситуаціях;

в) нормативне регулювання питань безпеки;

г) режим ділових зустрічей та переговорів;

г) взаємодія з правоохоронними органами;

д) навчальна підготовка особового складу СБ;

с) навчальна підготовка персоналу об’єкта з питань безпеки.

Такі служби охорони, як правило, створюються при місцевих органах внутрішніх справ або при державній службі безпеки. СБ будь-якої фірми постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі:

а) охорона виробничо-господарської діяльності та захист відомостей, що вважаються комерційною таємницею даного підприємства;

б) організація роботи з правового та інженерно-технічного захисту комерційних таємниць фірми;

в) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

г) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідного підприємства;

ґ) виявлення та локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та за екстремальних ситуацій;

д) організація режиму безпеки за здійснення всіх видів діяльності, включаючи зустрічі, переговори й наради в рамках ділового співробітництва підприємства з іншими партнерами;

е) забезпечення охорони приміщень, устаткування, офісів, продукції та технічних засобів, необхідних для виробничої або іншої діяльності;

є) організація особистої безпеки керівництва та провідних менеджерів і спеціалістів підприємства;

ж) оцінювання маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

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

- захист законних прав та інтересів суб'єктів підприємницької діяльності та їх співробітників;
- збирання даних, їх аналіз, оцінювання і прогнозування оперативної обстановки та різноманітних ризиків на підприємстві, в організації, установі;
- вивчення та перевірка партнерів, клієнтів і конкурентів;
- своєчасне виявлення можливих посягань на об'єкт чи його співробітників з боку джерел зовнішніх загроз безпеці;
- недопущення проникнення на об'єкт структур промислового шпіонажу, злочинних формувань чи осіб із протиправними намірами;
- протидія технічному проникненню на об'єкта чи його комунікаційні системи;
- захист співробітників об'єкта від насильницьких посягань;
- виявлення, запобігання можливій протиправній чи іншій негативній діяльності співробітників суб'єкта підприємництва на шкоду його безпеці;
- збереження матеріальних цінностей, відомостей з обмеженим доступом;
- пошук та здобування необхідної інформації для прийняття оптимальних управлінських рішень з питань стратегії і тактики подальшої підприємницької діяльності;
- фізичну і технічну охорону будов, споруд, територій, транспортних засобів;
- формування в засобах масової інформації у партнерів та клієнтури позитивного іміджу про суб'єкт підприємницької діяльності, що повинно сприяти реалізації бізнес-проектів;
- відшкодування матеріальних та моральних збитків, спричинених неправомірними діями юридичних чи фізичних осіб;
- організація і забезпечення пропускного та внутрішньо-об'єктного режиму в приміщеннях; порядок несення служби; контроль дотримання вимог режиму персоналом підприємства і партнерами (відвідувачами);
- участь у розробці основоположних документів (статуту, правил внутрішнього розпорядку, договорів тощо) з метою відображення в них вимог організації безпеки й захисту (комерційної таємниці):
- розробка та здійснення заходів із забезпечення роботи з документами, що містять відомості, які є комерційною таємницею, контроль виконання вимог матеріалів інструктивного характеру;
- виявлення і перекриття можливих каналів витоку конфіденційної інформації, облік та аналіз порушень режиму безпеки працівниками підприємства, клієнтами та конкурентами;
- організація та проведення службових розслідувань за фактами розголошення або втрати документів, інших порушень безпеки підприємства;
- розробка, оновлення і поповнення переліку відомостей, що становлять комерційну таємницю, та інших нормативних актів, які регламентують порядок організації безпеки й захисту інформації;
- забезпечення суворого виконання вимог нормативних документів з питань захисту комерційної таємниці;

- організація та регулярне проведення навчання працівників підприємства й служби безпеки за всіма напрямами захисту комерційної таємниці;
- ведення обліку сейфів і металевих шаф, якщо в них дозволене постійне чи тимчасове зберігання конфіденційних документів, а також облік та охорона спеціальних приміщень і технічних засобів;
- підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств (організацій) в інтересах вивчення криміногенної обстановки в районі;
- контроль за ефективністю функціонування системи безпеки.

У нормативних документах, які визначають організацію діяльності служб безпеки підприємств, виокремлюються конкретні об'єкти, які підлягають захисту від потенційних загроз і протиправних посягань. До них належать:
- персонал (керівники; персонал, який володіє інформацією, що становить комерційну таємницю підприємства);
- матеріальні цінності та фінансові кошти (приміщення, споруди, устаткування, транспорт; валюта, коштовні речі, фінансові документи);
- інформаційні ресурси з обмеженим доступом;
- засоби та системи комп'ютеризації діяльності підприємства;
- технічні засоби та системи охорони й захисту матеріальних та інформаційних ресурсів.

Лекція 5

4.2. Види і напрями діяльності установи, організації, підприємства

До основних завдань системи фінансово-економічної безпеки підприємства належать: захист законних прав і інтересів підприємства і його співробітників; збір, аналіз, оцінка даних і прогнозування розвитку обстановки; вивчення партнерів, клієнтів, конкурентів, кандидатів на роботу; виявлення, попередження і припинення можливої протиправної та іншої негативної діяльності співробітників підприємства на шкоду його безпеці; забезпечення збереження матеріальних цінностей і відомостей; отримання необхідної інформації для розроблення найбільш оптимальних управлінських рішень з питань стратегії і тактики економічної діяльності компанії тощо.

До основних елементів системи безпеки підприємства належать: 1) захист комерційної таємниці і конфіденційної інформації; 2) комп'ютерна безпека; 3) внутрішня безпека; 4) безпека будівель і споруд; 5) фізична безпека; 6) технічна безпека; 7) безпека зв'язку; 8) безпека перевезень вантажів і осіб; 9) екологічна безпека;10) конкурентна розвідка тощо.

Методика побудови системи економічної безпеки підприємства охоплює такі етапи:
- вивчення специфіки бізнесу підприємства, сегмента, який воно займає на ринку, штатного розпису, а також знайомство з персоналом;
- аналіз зовнішніх і внутрішніх загроз економічній безпеці підприємства та вивчення інформації про кризові ситуації, їхні причини і шляхи врегулювання;

- аудит наявних засобів із забезпечення безпеки й аналіз їх відповідності виявленим загрозам;

- моделювання нової системи економічної безпеки підприємства: розроблення плану усунення виявлених під час аудиту недоліків; підготовка пропозицій щодо удосконалення системи економічної безпеки (у т. ч. створення служби безпеки на підприємстві, якщо такої не існувало, чи системи безпеки на її базі, визначення механізмів її забезпечення та розроблення організаційної структури управління системою), розрахунок усіх видів необхідних ресурсів; планування щомісячних витрат на забезпечення функціонування системи економічної безпеки (бюджет);

- затвердження керівництвом моделі нової системи та бюджету на її утримання;

- формування нової системи фінансово-економічної безпеки;

- оцінка ефективності сформованої системи, а також її удосконалення.

Основне значення системи фінансово-економічної безпеки підприємства, організацій, установ полягає в тому, що вона повинна мати попереджувальний характер, а основними критеріями оцінки її надійності та ефективності є:

- забезпечення стабільної роботи підприємства, збереження і примноження фінансів і матеріальних цінностей;

- попередження кризових ситуацій, у тому числі різних надзвичайних подій, пов'язаних з діяльністю «зовнішніх» або «внутрішніх супротивників».

У режимі стійкого функціонування підприємство, організація, установа при вирішенні завдань економічної безпеки акцентує головну увагу на підтримці нормального ритму виробництва і збуту продукції, на запобіганні матеріальному чи фінансовому збитку, на недопущенні несанкціонованого доступу до службової інформації і руйнування комп'ютерних баз даних тощо. У кризові періоди розвитку найбільшу небезпеку для підприємства становить руйнування його потенціалу (виробничого, технологічного, науково-технічного і кадрового) як головного чинника життєдіяльності підприємства, його можливостей.

Головний комплекс проблем і основні причини поточного неблагополуччя багатьох промислових підприємств приховуються в: незатребуваності продукції на внутрішньому і зовнішньому ринках, у її низькій конкурентоспроможності; недоступності інвестиційних ресурсів; митних і валютних бар'єрах тощо. У цей час необхідне розроблення стратегії економічної безпеки, яке повинна містити:

- характеристику зовнішніх і внутрішніх загроз економічній безпеці підприємства;

- визначення і моніторинг чинників, що зміцнюють або руйнують стійкість його соціально-економічного положення на короткострокову і середньострокову перспективу;

- розроблення економічної політики, що охоплює механізми обліку, які впливають на стан економічної безпеки чинників; напрями діяльності підприємства щодо реалізації стратегії.

Організаційними заходами, що забезпечують реалізацію стратегії фінансово-економічної безпеки, є: 1) створення координаційного центру на чолі з керівником організації, оперативним органом якого є служба безпеки; 2) розроблення і затвердження наказом по підприємству нормативно-методичного забезпечення стратегії; 3) ресурсне забезпечення і цільове використовуванням ресурсів.

Комплексна система економічної безпеки підприємства має включати в себе комплекс взаємозв'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами суб'єкта господарювання, спрямованих на захист життєво важливих інтересів особистості, підприємства і держави від протиправних дій з боку реальних або потенційних фізичних або юридичних осіб, що можуть призвести до істотних економічних утрат та забезпечення економічного зростання в майбутньому. Отож, на основі викладеного матеріалу необхідно зазначити, що основними заходами, які необхідно здійснювати керівництву підприємства в процесі управління економічною безпекою, є наступні: формування необхідних корпоративних ресурсів (капіталу, персоналу, прав інформації, технології та устаткування); загально стратегічне прогнозування та планування економічної безпеки за функціональними складовими; стратегічне планування фінансово-господарської діяльності підприємства; загально-тактичне планування економічної безпеки за функціональними складовими; тактичне планування фінансово-господарської діяльності підприємства; оперативне управління фінансово-господарською діяльністю підприємства; здійснення функціонального аналізу рівня економічної безпеки; загальна оцінка досягнутого рівня економічної безпеки.

Тому, тільки при комплексному здійсненні в необхідному обсязі зазначених заходів вітчизняні підприємства зможуть досягти належного рівня своєї економічної безпеки.

Отже, досліджені аспекти економічної безпеки підприємства доводять необхідність формування системи її забезпечення на вітчизняних підприємствах, що зможе вплинути на ефективність їхнього функціонування у трансформаційній ринковій економіці.

4.3. Моделі економічної безпеки підприємства, установи, організації

У сучасних умовах господарювання включають наступні моделі економічної безпеки підприємства, установи, організації:

- структурно-логічна модель системи економічної безпеки, яка включає: захист інтересів організації у взаємодії з громадськістю; підтримка інтересів організації у системі державного, регіонального та місцевого управління; захист організації від економічних загроз; управління ефективністю та безпекою інвестиційної діяльності; забезпечення нормативно-правового захисту економічних інтересів; забезпечення фізичної безпеки майна та співробітників; управління ефективністю експлуатації економічних ресурсів; організація захисту комерційної таємниці; управління ефективністю та безпекою фінансування;
- модель свідомості – сукупність процедур і декларативних описів, за допомогою яких в інтелектуальних системах імітується частина свідомої людської діяльності, що має вербальний характер;
- функціональна модель – передбачає застосування механізмів концентрації та маневрування силами і засобами згідно з визначеними цілями і завданнями

з урахуванням змін у характері та інтенсивності загроз, що виникають;

- теоретична модель безпеки передбачає формування наукового структурно-логічного підходу до формування безпеки підприємств, організацій, установ;
- інструментальна модель – передбачає застосування інструментів захисту на підприємстві, організації, установі;
- комплексна модель – спрямована на застосування комплексу дій та засобів для забезпечення протидії зовнішнім і внутрішнім загрозам.

Питання для розгляду:

1. Охарактеризуйте види та напрями діяльності щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства.
2. Визначте моделі економічної безпеки на підприємстві, установі, організації.
3. Визначте завдання фінансово-економічної безпеки на підприємстві, організації, установі.
4. Назвіть функції служби безпеки.

Лекція 6

Тема 5. Технології інформаційно-аналітичного забезпечення діяльності підприємства, установи, організації. Технології, техніка та прийоми забезпечення фінансово-економічної безпеки підприємства, установи, організації. Аналіз процесів, які відбуваються на ринку (сегменті, в якому бере участь підприємство, установи, організації)

5.1. Технології інформаційно-аналітичного забезпечення діяльності підприємства, установи, організації. Технології, техніка та прийоми забезпечення фінансово-економічної безпеки підприємства, установи, організації.

5.2. Аналіз процесів, які відбуваються на ринку (сегменті, в якому бере участь підприємство, установи, організації).

Література: [36, 37, 36, 40, 44, 45, 46, 47, 55, 66].

5.1. Технології інформаційно-аналітичного забезпечення діяльності підприємства, установи, організації. Технології, техніка та прийоми забезпечення фінансово-економічної безпеки підприємства, установи, організації

В умовах розвитку інформаційного суспільства для розробки й впровадження стратегії необхідно сформувати й використовувати відповідне інформаційно-аналітичне забезпечення. У цьому контексті слід вказати, що для формування й обробки інформаційних потоків застосовуються широке коло інформаційного інструментарію, особливими з яких є Інтернет мережа. Особливе місце займають засоби масової інформації, які можуть формувати відношення заінтересованих

осіб до підприємств, їх продукції, проектів, корпоративної репутації.

Інформаційно-аналітичне забезпечення підприємства, банку розуміють сукупність юридичної, фінансової, ділової, технічної, технологічної та іншої інформації, яка перебуває в розпорядженні компанії, банку і використовується ними для забезпечення виробництва, проведення комерційних операцій, надання послуг, а також для управління їх діяльністю.

В основі формування інформаційних ресурсів лежать методи збору інформації, характерні для розвідувальної діяльності. Тому заходи інформаційно-аналітичного забезпечення діяльності підприємства, банку насамперед будуть ґрунтуватись на засадах комерційної розвідки. Водночас під комерційною розвідкою розуміють сукупність заходів щодо збору й обробки інформації про стан і можливі перспективи діяльності суб'єктів відповідного ринку, які виконуються за допомогою спеціальних методів силами комерційних підприємств, фірм, банків або спеціалізованих організацій (установ). Сьогодні комерційна розвідка в тому чи іншому обсязі здійснюється практично всіма підприємствами та банками. Більше того, результати розвідки значною мірою впливають на якість прийняття управлінських рішень, а отже, і на розвиток комерційних підприємств загалом. Тому комерційна розвідка є досить привабливою формою діяльності сил безпеки, але, враховуючи певну її особливість, ефективно реалізувати таку форму вдається далеко не всім.

Структуру комерційної розвідки складають організація розвідки, збір необхідних відомостей та інформаційно-аналітична робота. Ця структура являє собою сукупність взаємопов'язаних елементів розвідувальної системи, вилучення будь-якого з них веде до призупинення функціонування всієї системи.

Мета комерційної розвідки завжди спрямована на виконання двох умов діяльності комерційних підприємств, банків: а) виключення несподіваної появи несприятливих факторів для діяльності підприємства, банку і б) забезпечення об'єктивною інформацією прийняття відповідних рішень їх керівництвом. Об'єктами комерційної розвідки є передусім конкуруючі структури, підприємства, організації, які надають подібні послуги, виробляють аналогічні товари або у той чи інший спосіб впливають чи можуть впливати на діяльність даного підприємства, банку і в яких зосереджена або виробляється необхідна даному підприємству, банку інформація. В окремих випадках об'єктами комерційної розвідки також можуть бути технології виробництва товарів або послуг, комерційні операції.

Безпосереднє отримання інформації може здійснюватись через відповідні носії (джерела) такої інформації. Джерелами необхідної для комерційної розвідки інформації можуть бути люди (працівники відповідних установ, організацій, підприємств, банків, приватні детективи, інші категорії громадян, які з тих чи інших причин мають доступ до відповідної інформації), документи, засоби масової інформації, рекламні продукти, матеріали наукових досліджень, виробничі зразки, електронні носії інформації.

Організовуючи комерційну розвідку, необхідно чітко визначитись у правовому полі цієї діяльності: бізнесмен мусить достатньо чітко уявляти, в яких межах допускаються ті чи інші дії, коли ризик виправдовує засоби, а коли і не зовсім.

Пам'ятаючи про те, що в центрі всієї розвідувальної діяльності перебуває інформація, необхідно знати, що приблизно 70 % відомостей, що цікавлять

підприємця, можуть бути відкритими (публікуватися в пресі, рекламі, дайджестах та інших джерелах). Близько 15 % мають характер службової інформації, призначеної тільки для ознайомлення співробітників об'єкта. Це внутрішній розпорядок, пропускна система і система розмежування доступу, загальні правила роботи, вимоги щодо збереження комерційної таємниці, інформація про розташування об'єкта і його структуру, систему управління персоналом, принципи оплати праці та інша інформація, необхідна для забезпечення ефективного функціонування підрозділів об'єкта. Приблизно 10 % – відомості конфіденційного характеру, які в повному обсязі можуть доводиться тільки до керівного складу й осіб, безпосередньо пов'язаних з використанням їх у ході виконання своїх обов'язків. І тільки до 5 % відомостей є комерційною таємницею. Саме вони, як правило, найбільше цікавлять комерційну розвідку, хоча досягнення мети не завжди може виправдовувати затрачені зусилля.

Слід зауважити, що на сьогодні в Україні для комерційних підприємств, банків практично відсутні законні підстави для збору необхідної їм інформації, особливо такої, що має обмежений доступ (конфіденційної інформації, комерційної та банківської таємниці). Тому, організуючи діяльність комерційної розвідки, слід визначитись, яка саме інформація буде її об'єктом і які методи можуть застосовуватись для отримання певної інформації. Аналіз досвіду розвідувальної діяльності компаній іноземних країн показує, що в її організації чітко виявляються два напрямки: а) постійний моніторинг і аудит інформації, яка циркулює в інформаційному просторі і стосується діяльності та інтересів даної компанії; б) відповідні оперативні дії сил розвідки щодо додаткового збору інформації з метою забезпечення укладання конкретних комерційних угод, здійснення операцій, важливих комерційних заходів. Якраз такий підхід мало в чому порушує права власників інформації і забезпечує необхідну об'єктивність прийняття рішень. Подібним чином здійснюється діяльність комерційної розвідки і в країнах СНД, у тому числі і в Україні. Досвідчені бізнесмени, як правило, зосереджують діяльність своєї розвідки на роботі з джерелами відкритої інформації. Вони підбирають досить підготовлених з професійного погляду і досвідчених аналітиків і чітко визначають їхні завдання. Ці аналітики за допомогою глибокого вивчення й аналізу відкритих джерел отримують дуже цінні відомості про об'єкти, які їх цікавлять. Зазвичай таких відомостей буває достатньо для прийняття правильного рішення. У випадку, якщо інформації, отриманої у такий спосіб, недостатньо для глибокого і всебічного аналізу, може бути прийнято рішення про збір додаткових відомостей про об'єкт. У цьому разі визначають, які конкретно відомості необхідно отримати, де і хто може ними володіти, як їх можна роздобути і що для цього потрібно.

Тобто за існуючих в Україні умов розвідувальна діяльність комерційних підприємств, організацій, установ зосереджується в основному навколо інформаційно-аналітичної роботи і забезпечується шляхом збору інформації з відкритих джерел та її аналітичного дослідження.

5.2. Аналіз процесів, які відбуваються на ринку (сегменті, в якому бере участь підприємство, установи, організації)

До технологій, інструментів, засобів формування й використання інформаційно-аналітичного забезпечення у рамках стратегії фінансово-економічної безпеки на підприємстві відносять:

- визначення сфер та об'єктів інформаційної уваги підприємства, банку;
- визначення мети і завдань інформаційно-аналітичної роботи (ІАР);
- підбір (підготовку) сил і засобів для проведення заходів ІАР;
- планування роботи;
- визначення і постановку завдань виконавцям;
- забезпечення заходів ІАР;
- контроль діяльності сил і засобів, залучених до виконання завдань ІАР.

Збір інформації передбачає вжиття таких заходів:

- створення інформаційних каналів;
- вибір об'єктів інформації, визначення і придбання (отримання) її джерел;
- організація роботи з інформаційними джерелами, отримання (споживання) інформації;
- забезпечення безперервної роботи джерел інформації.

Обробка інформації забезпечується через:

- накопичення, оцінювання та аналіз інформації;
- класифікацію інформації, її зіставлення та перевірку достовірності, вилучення необ'єктивних і суперечливих відомостей;
- формування гіпотез;
- інтерпретації інформації;
- створення інформаційних баз даних;
- розподіл інформації, розроблення інформаційних документів.

Отримання інформації у сферах інформаційної уваги здійснюється через відповідні канали:

1. Інформаційний канал ТЕКСТ – загальні публікації, спеціальні публікації, бази даних. Характеристика каналу: наявність великих обсягів «свіжої», але не зовсім об'єктивної інформації. Місткість каналу – 40-60 % необхідної інформації.

2. Інформаційний канал БАНК, ФІРМА – персонал, клієнти, партнери. Характеристика каналу: технологічна, ділова інформація, інформація про окремих суб'єктів та окремі події, приблизно об'єктивна. Місткість каналу – 30-40 % необхідної інформації.

3. Інформаційний канал КОНСУЛЬТАНТ – нормативні документи, експерти, радники, консультанти, органи управління, політичні та громадські організації. Характеристика каналу: достовірна інформація. Місткість каналу – 10-15 % необхідної інформації.

4. Інформаційний канал БЕСІДА – всі види ділового спілкування: конференції, семінари, переговори, зустрічі, презентації, виставки, наради. Характеристика каналу: достовірна інформація на перспективу. Місткість каналу – 5 % необхідної інформації.

5. Інформаційний канал «ДЖОКЕР» (випадок) – випадкова інформація.

Місткість каналу 0-100 % необхідної інформації.

Основними заходами інформаційно-аналітичної роботи банків є інформаційний аудит та інформаційний моніторинг. Під інформаційним аудитом розуміють проведення інформаційних досліджень підрозділів і установ банку з метою вивчення й оцінки інформації, яка в них є. У ході інформаційного аудиту вивчається склад інформації підрозділів та установ, джерела, форми і регламент отримання ними інформації, можливості інформації для трансформації її в інші види (ділову, фінансову і т. п. або ж в стратегічну, тактичну, оперативну), ступінь захисту інформації. Крім того, відбирається інформація для формування інформаційних баз даних.

Під час інформаційного моніторингу проводиться контроль отримання підрозділами й установами банку інформації, появи нової інформації в інформаційному середовищі банку, визначається її цінність і важливість для формування інформаційних ресурсів та забезпечення його безпеки. Уході моніторингу здійснюються: оцінка інформації та її розподіл за інформаційними базами даних, виявлення неправдивої або шкідливої інформації та визначення джерел надходження такої інформації, формування інформаційних потоків залежно від завдань, які вирішує банк. У процесі інформаційного моніторингу забезпечується своєчасна реакція на зміни в інформаційних каналах та пошук додаткових джерел інформації.

Інформаційно-аналітична робота у загальному вигляді спрямована на створення моделі відповідного об’єкта (людина, фірма, виробництво), діяльності (банківські операції, взаємовідносини суб’єктів на ринку банківських послуг), стану (рівень розвитку, основні показники) тощо на основі отримання та аналізу інформації. Створення таких моделей є продуктом інтелектуальної діяльності конкретної людини, фахівця служби безпеки. Модель як погляд на подію у кожної людини своя. До того ж як би вона не була близька до дійсності, все одно буде суб’єктивною. Залежно від індивідуальних особливостей психічного відображення реальності у людей переважатимуть ті чи інші моделі. Їх неможливо розглядати з позиції «хороші» вони чи «погані». Моделі треба розглядати в контексті того, чи відповідають вони фактичним діям об’єкта й умовам його існування. Людина не чинить неправильно, просто у неї буває обмежена кількість варіантів рішень. Тому модель може бути більше або менше наближеною до об’єктивного стану об’єкта.

У побудові моделі беруть участь дві групи процесів психічного відображення:

- процеси, що забезпечують інформацією про властивості середовища перебування об’єкта, – відчуття і сприйняття;
- процеси, що забезпечують перероблення і збереження інформації та побудову моделі, – мислення і пам’яті.

І все ж таки модель як результат інформаційно-аналітичної роботи заздалегідь приречена на суб’єктивність як у наслідок спотворення інформації у ході її сприйняття, так і в результаті специфіки розумових процесів індивідуума при обробці інформації, що характерно для різних психологічних типів людей. Під час побудови моделі економічної безпеки використовується ряд специфічних прийомів:

- порівняння – процес, який забезпечує первинну оцінку інформації на основі зіставлення її елементів з відомими нам моделями і знаходження схожості між ними;

- аналіз – процес розподілу відображеної у вигляді предметів, подій, явищ інформації на складові елементи з подальшим детальним розглядом окремих їх властивостей. У забезпеченні цього процесу провідна роль відводиться свідомості й підсвідомості;

- синтез – об'єднання групи властивостей, які притаманні відповідному предмету, об'єкту, в єдине ціле, створення моделей відомих нам об'єктів, процесів і явищ (стану, діяльності) з окремих елементів, прогнозування розвитку в часі, прогнозування поведінки окремих людей;

- узагальнення – ідентифікація раніше невідомих об'єктів, явищ із уже відомими за якими-небудь загальними ознаками. В узагальненні міститься як корисний, так і небезпечний компонент. Корисний – можливість об'єднання предметів і явищ у великі групи на основі невеликих груп базових ознак. Але при цьому з'являється загроза перекручення об'єктивного стану цих предметів і явищ у наслідок дуже великого скорочення незначних ознак узагальнюючої моделі;

- виключення – процес, у якому звертається увага на відповідні аспекти особистого досвіду аналітика і виключаються інші. Це дає змогу в ситуаціях, які часто повторюються, швидко знаходити необхідну форму реакції, концентруючи увагу на якій-небудь відповідній частині доступного досвіду.

Така властивість дає можливість виключити надходження до свідомості зайвих зовнішніх стимулів:

- абстрагування – розгляд предмета, явища, елемента інформації відірвано від будь-якої реальності;

- трансформація – перетворення інформації, що сприймається, відповідно до моделі, яку формують. Трансформація лежить в основі фантазії, прогнозу, будь-якої творчої діяльності.

Створена в результаті інформаційно-аналітичної роботи модель об'єкта, діяльності, стану чи окремої події не є закінченою. Її слід доповнювати новими даними та новою інформацією.

Таким чином, інформаційно-аналітичне забезпечення діяльності банків насамперед спрямоване на створення їх інформаційного ресурсу і відповідної системи інформування керівництва та за його вказівкою інших працівників банків, а також на проведення інформаційних досліджень суб'єктів у сфері інформаційної уваги банків.

Питання для розгляду:

1. Охарактеризуйте напрями інформаційно-аналітичного забезпечення діяльності підприємства, установи, організації.
2. Визначте технології інформаційно-аналітичного забезпечення діяльності підприємства, установи, організації.
3. Охарактеризуйте канали забезпечення інформаційного захисту.
4. Назвіть прийоми, які використовуються для забезпечення економічної безпеки.

Лекція 7

Тема 6. Стратегія діяльності підприємства, установи, організації. Стратегія розвитку установи, організації, підприємства. Стратегія фінансово-економічної безпеки підприємства, установи, організації. Стратегія забезпечення фінансово-економічної безпеки підприємства, установи, організації. Перспективні та поточні плани щодо забезпечення фінансово-економічної безпеки підприємства, установи, організації

6.1. Стратегія діяльності підприємства, установи, організації. Стратегія розвитку установи, організації, підприємства. Стратегія фінансово-економічної безпеки підприємства, установи, організації. Стратегія забезпечення фінансово-економічної безпеки підприємства, установи, організації.

6.2. Перспективні та поточні плани щодо забезпечення фінансово-економічної безпеки підприємства, установи, організації.

Література: [13, 14, 16, 17, 20, 22, 23, 24, 25, 34, 35, 38, 53, 57, 58, 61, 62, 63, 64, 68, 72, 73, 77, 78, 79, 80, 81].

6.1. Стратегія діяльності підприємства, установи, організації. Стратегія розвитку установи, організації, підприємства. Стратегія фінансово-економічної безпеки підприємства, установи, організації. Стратегія забезпечення фінансово-економічної безпеки підприємства, установи, організації

Визначення та напрями визначення й розробки стратегії підприємства, установи, організації, його розвитку представлені в темі 1 представленого конспекту лекції.

Стратегія забезпечення й реалізації фінансово-економічної безпеки на підприємстві, установі, організації включає наступні етапи:

1. Формування інформаційно-аналітичного забезпечення щодо створення й реалізації фінансово-економічної безпеки на підприємстві, організації, установи, яке повинно відповідати повноті, достовірності, ціле орієнтованості та ін.

2. Характеристика інструментарію, моделей, методів для формування й реалізації фінансово-економічної безпеки на підприємстві, установі, організації.

3. Формування та трансформація організаційних підрозділів на підприємствах, організаціях, установах.

4. Визначення джерел фінансування щодо формування та реалізації фінансово-економічної безпеки на підприємстві, організації, установі.

5. Характеристика точок зростання та проблемних аспектів щодо формування та реалізації фінансово-економічної безпеки на підприємстві, організації, установі.

6. Моніторинг і контроль за формуванням і реалізацією заходів щодо формування та реалізації заходів щодо фінансово-економічної безпеки.

7. Реалізація заходів щодо формування і використання фінансово-економічної безпеки на підприємстві, організації, установі.

6.2. Перспективні та поточні плани щодо забезпечення фінансово-економічної безпеки підприємства, установи, організації

Перспективні та поточні плани щодо забезпечення фінансово-економічної безпеки підприємства, установи, організації представляють собою сукупність взаємопов'язаних дій, які спрямовані на забезпечення фінансово-економічної безпеки шляхом протидії зовнішнім і внутрішнім загрозам.

Для розробки перспективних та поточних планів щодо забезпечення фінансово-економічної безпеки визначаються і характеризуються відповідні складові:

- Фінансова складова вважається провідною й вирішальною для ефективного функціонування підприємства. До фінансової складової економічної безпеки входять такі елементи, за якими оцінюється стан загрози: аналіз загрози негативних дій щодо політико-правової складової економічної безпеки; оцінка поточного рівня забезпечення фінансової складової економічної безпеки; оцінка ефективності запобігання можливій шкоді від негативних дій, пов'язаних з антикризовими явищами; планування комплексу заходів і розробки рекомендацій щодо фінансової складової економічної безпеки.
- Інтелектуальна і кадрова складова визначає в першу чергу інтелектуальний та професійний склад кадрів. План інтелектуальної та кадрової складових економічної безпеки має охоплювати як взаємопов'язані, так і самостійні напрями діяльності того чи іншого суб'єкта господарювання. У плані має бути визначений можливий негативний вплив антикризових факторів за наявності працівників чи структурних підрозділів, які не здатні приносити максимальну користь своєму підприємству. План має бути спрямований на охорону належного рівня безпеки й охоплювати організацію системи підбору, найму, навчання й мотивації праці працівників, включаючи матеріальні та моральні стимули, престижність професії, свободу творчості, забезпечення соціальними благами.
- Техніко-технологічна складова передбачає аналіз ринку технологій стосовно виробництва продукції аналогічного профілю певного підприємства.
- Політико-правова складова охоплює такі елементи організаційно-економічного спрямування: 1) аналіз загроз негативних впливів; 2) оцінку поточного рівня забезпечення; 3) планування (програму) комплексних заходів спеціалізованими підрозділами підприємства; 4) здійснення ресурсного планування; 5) планування роботи відповідних функціональних підрозділів підприємства.
- Інформаційна складова економічної безпеки формується таким чином: 1) здійснюється збір всіх видів інформації, яка стосується діяльності суб'єкта господарювання; 2) аналіз отриманої інформації з дотриманням загальноприйнятих принципів (систематизації, безперервності надходження, характеру аналітичних процесів) і методів (локальних і специфічних проблем,

загально корпоративних проблем) організації робіт; 3) прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на підприємстві, в країні, за кордоном стосовно конкретної сфери бізнесу; 4) оцінювання рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення рівня безпеки на конкретному суб'єкті господарювання; 5) збір інших видів інформації, спрямованої на антикризову діяльність (зв'язок з громадськістю, формування іміджу підприємства, захист конфіденційної інформації). Весь комплекс інформаційної складової є важливим фактором для своєчасного прийняття правильного рішення з боротьби з можливими проявами кризових ситуацій.

- Екологічна складова має гарантувати безпеку суспільству від суб'єктів господарювання, що здійснюють виробничо-комерційну діяльність. З цією метою товаровиробник повинен ретельно дотримуватись національних норм мінімально допустимого вмісту шкідливих речовин, що потрапляють у навколишнє середовище, та екологічних параметрів продукції, яка виготовляється. План забезпечення екологічної складової є частиною загальної антикризової програми і економічної безпеки підприємства.
- Силова складова економічної безпеки в програмі антикризового господарства має: забезпечити фізичну і моральну безпеку співробітників; гарантувати безпеку майна та капіталу підприємства; гарантувати безпеку інформаційного середовища підприємства; забезпечити сприятливе зовнішнє середовище бізнесу.

Питання для розгляду:

1. Охарактеризуйте напрями розробки та етапи реалізації стратегії фінансово-економічної безпеки підприємства, установи, організації.
2. Охарактеризуйте складові фінансово-економічної безпеки.

Змістовий модуль 3
Розробки й впровадження перспективних планів фінансово-економічної безпеки в сфері стратегічного та інноваційного менеджменту

Лекція 8

Тема 7. Положення про службу безпеки підприємства, установи, організації. Технології захисту передачі інформації. Оцінка діяльності щодо впровадження сучасних технологій забезпечення економічної безпеки та попередження ризиків та загроз

7.1. Положення про службу безпеки підприємства, установи, організації.
7.2. Технології захисту передачі інформації.
7.3. Оцінка діяльності щодо впровадження сучасних технологій забезпечення економічної безпеки та попередження ризиків та загроз.

Література: [72, 73, 74, 75, 76, 85].

7.1. Положення про службу безпеки підприємства, установи, організації

Для розробки стратегії щодо забезпечення фінансово-економічної безпеки підприємства, установи, організації необхідно сфокусувати увагу на Положенні про службу безпеки на підприємстві, організації, установі.

Служба безпеки (СБ) підприємства створюється наказом директора з метою захисту економічних інтересів підприємства і забезпечення максимальної безпеки його діяльності як суб'єкта ринкових відносин.

Служба безпеки є самостійним підрозділом і підпорядковується безпосередньо керівнику підприємства.

Керівництво службою здійснює начальник СБ, що призначається і звільняється від займаної посади керівником підприємства.

Структура і штати СБ за поданням її начальника затверджуються керівником підприємства.

Діяльність СБ фінансується за рахунок включення її витрат у собівартість робіт, виконуваних підприємством.

Служба безпеки у своїй діяльності керується законами України, указами Президента, постановами Кабінету Міністрів, відомчими наказами і вказівками, Статутом підприємства, наказами і вказівками керівника підприємства і внутрішнім Положенням про СБ.

У залежності від виду підприємницької діяльності, розмірів фірми й інших критеріїв її функціонування набір елементів механізму захисту підприємницької таємниці може кардинально змінюватися, що відображається в Положенні про службу безпеки. Звичайно, важливу роль відіграють й фінансово-матеріальні можливості, необхідні для організації захисту економічної безпеки.

Як правило, для комплексного вирішення всіх питань, пов'язаних із захистом підприємницької таємниці, на фірмі створюється власна служба безпеки, начальник якої є і заступником керівника фірми. Однак окремими питаннями захисту економічної безпеки можуть займатися спеціалізовані охоронні підприємства, що виконують свої функції за договором із фірмою.

У Положенні про службу безпеки визначено:

- організація й забезпечення пропускного і внутріоб'єктного режиму в будинках і приміщеннях, несення їхньої охорони, контроль за дотриманням установленого режиму на фірмі співробітниками, відвідувачами;
- проведення заходів щодо правового й організаційного регулювання відносин на фірмі по захисту підприємницької таємниці й економічної безпеки;
- участь у розробці основних нормативних документів (інструкцій, положень), що встановлюють порядок і принципи захисту підприємницької таємниці;
- участь у розробці посадових інструкцій, обов'язків керівників підрозділів, фахівців, усіх категорій працівників;
- забезпечення збереження документів, що містять зведення, що є комерційною таємницею, припинення їхнього розкрадання або передачі зведень зацікавленим

особам іншими способами;

- організація проведення службових розслідувань по фактах розголошення зведень, що складають підприємницьку таємницю, втрат документів і інших порушень безпеки фірми, а також і інші функції, що повинні бути встановлені в положенні про службу безпеки, затвердженому керівником фірми.

Відповідно до Положення про службу безпеки, характеризується механізм безпеки, до складу якого входять наступні підсистеми:

- правове забезпечення таємниці;
- правознавство організаційного захисту;
- здійснення інженерно-технічного захисту;
- мотивація в першу чергу тих співробітників, від поводження яких залежить витік зведень, що складають підприємницьку таємницю;
- посилення різних форм відповідальності за розголошення зведень, що наносять економічний збиток фірмі тощо.

Особливе значення має організація інженерно-технічного захисту, що являє собою сукупність спеціальних інженерно-технічних засобів, застосування яких забезпечує безпека фірми, її майна, ресурсів, а також зведень про діяльність підприємства, організації, установи.

Основними задачами СБ підприємства є:

1. Забезпечення економічної безпеки, захисту власності підприємства.
2. Організація діловодства.
3. Забезпечення заходів захисту при використанні засобів зв'язку (телетайп, телекс, телефакс, телефон, комп'ютерні мережі, супутниковий зв'язок).
4. Організація протидії технічним засобам розвідки на об'єктах підприємства.
5. Забезпечення всередині об'єктового і пропускного режиму, охорона майна і персоналу підприємства, фізична охорона вищого керівництва фірми (та інших співробітників у разі потреби: касири, інкасатори, науковці, технологи, інженери тощо).
6. Забезпечення захисту охоронюваної інформації й економічної безпеки при здійсненні зовнішньоекономічної діяльності.
7. Надання допомоги структурним підрозділам у вивченні кон'юнктури ринку, передбачуваних партнерів, конкурентів, посадових осіб різних гілок влади.
8. Контроль за виконанням нормативних документів.
9. Виявлення і закриття можливих каналів витоку охоронюваної інформації в процесі виробничої й іншої діяльності підприємства.
10. Контроль за станом протипожежної безпеки на об'єктах підприємства.

Відповідно до основних задач СБ підприємства виконує наступні функції:

1. З питань допуску співробітників до охоронюваної інформації:

- Спільно з фахівцями – відповідальними виконавцями розробляє перелік зведень, що складають комерційну таємницю підприємства. Вносить відповідні документи на розгляд і затвердження керівником. Контролює відповідність змісту й умов проведення робіт реквізиту «КТ-власність підприємства» і терміни його дії.
- Розробляє і здійснює заходи, що забезпечують доступ до охоронюваної інформації тільки тим особам, яким це необхідно для виконання службових

обов’язків.

- Розробляє систему організаційних і технічних заходів, що регламентують усередині об’єктовий режим підприємства. Організовує і контролює їх виконання.
- Здійснює контроль за виготовленням, обліком, збереженням, видачею і використанням бланків службових посвідчень (пропусків), печаток, штампів підприємства, а також металевих і мастичних печаток з індивідуальними обліковими номерами.

2. З питань діловодства:

- Організовує і веде діловодство; контролює забезпечення встановленого порядку розмноження документів, їхнього обліку, збереження і користування ними, а також знищення.
- Забезпечує дотримання правил розсилання документів, які містять комерційну таємницю підприємства.
- Розробляє і здійснює заходи для запобігання розголошення і витоку інформації при веденні діловодства.

3. З питань передачі і прийому інформації технічними засобами зв’язку:

- Організовує прийом і передачу охоронюваної інформації і відкритої кореспонденції по телекомунікаційним каналам (телетайпу, телексу, телефаксу тощо).
- Вибирає ефективні й економічні засоби зв’язку в залежності від характеру переданої інформації. Враховує й аналізує вхідну і вихідну кореспонденцію, оперативно доводить до адресатів.

4. З питань забезпечення пропускного режиму, охорони майна і персоналу підприємства, контролю за протипожежною безпекою:

- Розробляє документи, що регламентують пропускний режим і затверджує їх у керівника підприємства. Оформляє, враховує, видає, вилучає усі види пропусків на територію підприємства. Контролює правильність оформлення документів на ввіз (вивіз), внесення (винос) матеріальних цінностей і документів.
- Організує контрольно-пропускні пости (пункти). Забезпечує встановлений часовий режим охорони об’єктів підприємства. Експлуатує технічні засоби охорони.
- Розробляє і здійснює заходи для забезпеченню особистої безпеки працівників підприємства.
- Стежить за станом протипожежної безпеки, пропонує заходи для усунення порушень.

5. З питань інженерно-технічного забезпечення безпеки охоронюваної інформації й охорони підприємства:

- Розробляє вимоги до приміщень, де ведуться роботи з охоронюваною інформацією, зберігаються відповідні документи, вироби, а також матеріальні цінності. Проводить атестацію приміщень і об’єктів збереження матеріальних цінностей. Організовує установку й експлуатацію технічних засобів захисту, у тому числі і засобів протидії технічним розвідникам.
- Координує заходи безпеки при проведенні робіт з використанням електронно-обчислювальної техніки та телекомунікаційних засобів. Організовує спец перевірки та спец дослідження. Контролює виконання нормативних документів при експлуатації ПЕОМ та їх мереж.

- Веде облік сейфів, металевих шаф, спеціальних сховищ (а також ключів чи машино зчитуваних карток до них), у яких дозволено постійно або тимчасово зберігати документи, що містять охоронювану інформацію (з реквізитом «КТ-власність підприємства»).

- Контролює виконання заявок (договорів) на установку і ремонт інженерно-технічних засобів захисту, а також установку засобів зв'язку.

6. З питань безпеки інформації при здійсненні зовнішньоекономічної діяльності:

- Бере участь у доборі фахівців, здатних вести ефективну реготу із закордонними фірмами й у підготовці оформлення виїзних документів для зарубіжних відряджень.

- Бере участь у підготовці документів і матеріалів (програми, угоди, контракти) із зовнішньоекономічної діяльності, організації переговорів, прийомів і іншими спільних із закордонними фахівцями заходів на території підприємства і поза нею.

7. Надає методичну допомогу відповідальним виконавцям з питань забезпечення економічної безпеки при укладанні договорів зі сторонніми організаціями.

8. Бере участь в експертизі матеріалів, підготовлених до відкритої публікації (статті, доповіді, реклама тощо).

9. Здійснює організаційно-методичне керівництво уповноваженими по захисту комерційної таємниці в структурних підрозділах. Проводить консультації для співробітників підприємства з організаційно-правових питань забезпечення економічної безпеки і способів захисту охоронюваної інформації.

10. Із залученням фахівців підприємства вивчає всі види діяльності підрозділів з метою виявлення її закриття можливих каналів витоку охоронюваної інформації і нанесення економічного збитку.

11. Організує службові розслідування по фактах розголошення охоронюваної інформації, втрати документів або виробів, що містять такі зведення, порушень внутрішньо-об'єктового і пропускного режиму підприємства.

12. Здійснює зв'язок із правоохоронними й іншими державними органами з питань захисту комерційної таємниці і забезпечення економічної безпеки підприємства.

Структура служби безпеки на підприємстві, установі, організації:

1. Виходячи із задач і функцій у СБ підприємства входять:

- Підрозділ захисту інформації.
- Підрозділ технічних засобів зв'язку і протидії технічним засобам розвідки.
- Підрозділ охорони.

2. Задачі, функції, права, відповідальність структурних ланок СБ визначаються окремими положеннями і посадовими інструкціями її співробітників.

7.2. Технології захисту передачі інформації

Сукупність технологій захисту передачі інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи.

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та

інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Програмні методи захисту – це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи.

Лише комплексне використання різних заходів може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

У якості технологій захисту передаваємої інформації використовуються:

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Документом, який засвідчує чинність і належність відкритого ключа підписувачу, є сертифікат відкритого ключа (далі – сертифікат ключа), виданий центром сертифікації ключів.

Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача.

Сертифікат ключа, що засвідчує відкритий ключ підписувача, згідно зі ст. 6 Закону містить такі обов'язкові дані:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
- зазначення, що сертифікат виданий в Україні;
- унікальний реєстраційний номер сертифіката ключа;
- основні дані (реквізити) підписувача – власника особистого ключа;

- дату і час початку та закінчення строку чинності сертифіката;
- відкритий ключ;
- найменування криптографічного алгоритму, що використовується власником особистого ключа;
- інформацію про обмеження використання.

Для ефективної передачі інформації система має працювати в реальному масштабі часу, тому необхідно оперативне виявлення перекручувань інформації та її наслідків, а також оперативне й автоматичне вживання заходів щодо ліквідації чи зменшенню можливих відхилень процесу передачі від нормального режиму без його зупинки чи тривалого переривання. При цьому повинна враховуватися тривалість прояву наслідків перекручування в результатах функціонування системи і застосовуватися корегування ходу процесу, що забезпечує максимальне скорочення тривалості прояву цих наслідків. Для забезпечення захисту процесу передачі інформації використовується інформаційна і часова надмірність. При цьому під часовою надмірністю системи розуміють можливість використання деякої частки продуктивності системи для контролю виконання програм. Для цього при проектуванні системи повинен передбачатися запас продуктивності, що буде використовуватися для оперативного контролю і підвищення надійності функціонування. Величина часової надмірності залежить від вимог до надійності функціонування системи і знаходиться звичайно в межах від 5-10 % продуктивності простої системи (один рівень перевірки) до двох, трьох і чотирьох разового дублювання продуктивності в складних системах (багаторівневі перевірки).

Часова надмірність чи резерв часу використовується для контролю і виявлення перекручувань, на його перевірку та ухвалення рішення по відновленню процесу передачі на реалізацію операцій відновлення.

Для більшості систем передачі інформації, які працюють у реальному масштабі часу, необхідні досить висока вірогідність і безперервність генерування інформаційних впливів. Тому неприпустимі значні перерви і перекручування у видаванні тестів. Для виконання цих умов спеціалісти змушені вживати спеціальних заходів захисту від перекручувань, виходячи з припущення, що вони можуть з’явитися у будь-який момент. При цьому, насамперед, варто вжити заходів захисту від помилок, що найбільше спотворюють вихідні результати і не дозволяють системі виконувати свої функції.

Існує досить багато методів захисту процесу передачі. Розглянемо захист від зациклювання тестів. У діагностичних тестах широко використовуються однотипні діагностичні операції, що утворять цикли для пошуку, упорядкування й однотипного перетворення інформації. Причиною зациклення можуть бути не тільки помилки в тесті й перекручування вихідної інформації, але і збої в апаратурі комп’ютерної системи. Тому при виявленні первинного зациклення доцільно повторити включення тестів при тих же вихідних даних. Якщо зациклення не повторюється, то, швидше за все, воно відбулося в результаті випадкового збою. Повторне зациклення при однакових вихідних даних може бути обумовлено помилкою в тесті при правильної вихідної інформації, перекручуванням вихідної чи інформації частковим відмовленням апаратури. При багаторазових зацикленнях з різними вихідними даними причиною є, швидше за все, часткове відмовлення

в апаратурі чи перекручування інформації про процес передачі інформації.

Оперативний захист від перекручувань інформації й обчислювального процесу може використовуватися як засіб виявлення помилок які складно виявляються. Це особливо необхідно на завершальних етапах перевірки передачі й у процесі експлуатації даної комп'ютерної системи. Головна задача забезпечення стійкості та оперативного захисту від різних перекручувань складається в забезпеченні безперервності процесу керування комп'ютерною системою при припустимих помилках у вихідних повідомленнях системи. В системі використовуються наступні міри для забезпечення стійкості процесу передачі інформації: відновлення інформації і збереження стійкості процесів передачі, ігнорування виявленого перекручування внаслідок його слабкого впливу на весь процес передачі і на вихідні результати, повторення функціонального алгоритму чи тесту при тих же вихідних даних, виключення тесту з обробки внаслідок його перекрученості чи труднощів відновлення процесу передачі, короткочасне припинення рішення задач даного функціонального алгоритму до відновлення вихідних даних, перебудова режиму роботи алгоритму для зниження впливу перевантаження в зв'язку з втратою інформації про хід процесу передачі інформації.

7.3. Оцінка діяльності щодо впровадження сучасних технологій забезпечення економічної безпеки та попередження ризиків та загроз

Оцінка діяльності щодо впровадження сучасних технологій забезпечення фінансово-економічної безпеки та попередження ризиків і загроз здійснюється на основі інформаційно-аналітичного забезпечення моніторингу фінансово-економічної безпеки, яке розглядається як сукупність заходів щодо збору й обробки інформації про стан і можливі перспективи діяльності підприємств, установ, організацій у всіх сферах інформаційної уваги на стратегічному, оперативному та тактичному рівнях з метою своєчасного попередження та викриття на ранній стадії загроз, а також отримання необхідної інформації для планування, підготовки і проведення заходів з метою усунення можливих противоправних дій.

Як правило, підприємства забезпечують роботу своїх сил безпеки у всіх сферах інформаційної уваги і використовують інформацію: у сферах інтересів – як стратегічну для прийняття рішень щодо довгострокових угод, договорів, планування перспектив розвитку підприємства; у сферах впливу – як тактичну для прийняття рішень щодо співробітництва з партнерами, інвестування (вкладання) коштів у нові проекти, протидії недобросовісній конкуренції, визначення поведінки на ринку в той чи інший проміжок часу; у сферах безпосередньої інформаційної діяльності – як оперативну для прийняття рішень щодо безпосереднього здійснення конкретної операції, укладання конкретної угоди.

Для оцінки рівня фінансово-економічної безпеки корпоративного підприємства запропоновано враховувати такі параметри: інтегральна оцінка рівня фінансово-економічної безпеки корпоративного підприємства; коефіцієнт ризикованості зовнішнього середовища; коефіцієнт ризикованості внутрішнього

середовища. Інтегральну оцінку рівня фінансово-економічної безпеки здійснюють за двома складовими: рівень інформаційної захищеності та забезпечення безпеки інформаційних ресурсів в системі корпоративного управління підприємств будівельної галузі та інтегральних параметрів фінансово-економічного стану підприємства.

Основним критерієм відбору переліку індикаторів слугує рівень вразливості окремих сфер функціонування корпоративного підприємства, а також найбільший ступінь впливу окремих дестабілізуючих чинників на реалізацію окремих корпоративних інтересів.

Для оцінки рівня інформаційної захищеності та забезпечення безпеки інформаційних ресурсів, оцінки діяльності щодо впровадження сучасних технологій забезпечення економічної безпеки та попередження ризиків і загроз в системі управління підприємств сформовано компоненти: інформаційна політика та забезпечення безпеки інформаційних ресурсів; рівень обов'язкового (необхідного та достатнього) розкриття інформації; рівень розкриття додаткової інформації про діяльність підприємства; рівень достовірності інформації, що розкривається; своєчасність розкриття інформації; рівень зручності поширення інформації; рівень захисту внутрішньої інформації. Оцінювання ступеню впливу інтегральних показників інформаційної захищеності здійснено за методом Дельфі.

Формується інтегрований компонент фінансово-економічного стану підприємств за даними фінансової і статистичної звітності підприємств, установ, організації. Інтегральні показники визначаються шляхом адитивної згортки індикаторів кожної компоненти.

Питання для розгляду:

1. Охарактеризуйте Положення про службу безпеки підприємства, установи, організації.
2. Визначте розділи Положення про службу безпеки підприємства, установи, організації.
3. Охарактеризуйте розділи Положення про службу безпеки підприємства, установи, організації.
4. Які технології використовуються для захисту інформації.
5. Охарактеризуйте напрями оцінки діяльності щодо впровадження сучасних технологій забезпечення економічної безпеки та попередження ризиків та загроз.

Лекція 9

Тема 8. Розподіл повноважень і відповідальності між структурними підрозділами в системі безпеки установи, організації, підприємства. Система оцінювання роботи працівників з реалізації політики, програм і планів щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства

8.1. Розподіл повноважень і відповідальності між структурними підрозділами в системі безпеки установи, організації, підприємства.
8.2. Система оцінювання роботи працівників з реалізації політики, програм і планів щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства.

Література: [32, 48, 49, 50, 54, 59, 60, 69].

8.1. Розподіл повноважень і відповідальності між структурними підрозділами в системі безпеки установи, організації, підприємства

Для забезпечення розподілу повноважень і відповідальності між структурними підрозділами в системі безпеки установи, організації, підприємства визначаються нормативними актами, які регламентуються організацією взаємодії та повноважень і відповідальність на підприємстві, відносяться положення про структурні підрозділи і посадові інструкції працівників. Основні функції структурних підрозділів, межі компетентності їх менеджерів визначає перший керівник підприємства.

Документами, що встановлюють відповідальність та визначають напрями функціонування організаційних підрозділів щодо забезпечення фінансово-економічної безпеки на підприємстві, установі, організації є положення про структурний підрозділ, посадові інструкції.

Правильно розроблені положення сприяють поліпшенню організації управління, підвищенню ефективності праці управлінського персоналу, укріпленню дисципліни, опрацюванню більш якісних управлінських рішень.

Встановлюючи функції підрозділів і компетенцію їх керівників, перший керівник, окрім об’єктивних факторів (обсяг робіт, чисельність і підготовка персоналу, порядок роботи), враховує особисту, суб’єктивну оцінку діяльності керівників підрозділів, їх провідних фахівців. Виходячи з цього, розробляють положення про підрозділи, що визначають нормативно-правову регламентацію їх діяльності.

Положення про підрозділи розробляються з урахуванням таких рекомендацій:

1) вони повинні бути конкретними, а формулювання, які містяться в них, чіткими й однозначними;

2) складати їх слід за єдиною методикою керівникам підрозділів за умови допомоги з боку служби, яка забезпечує розробку й розв’язання питань організації

й управління;

3) положення мають бути погоджені між собою;

4) при розробці положень слід додержуватися принципу системності, який полягає в тому, що складання положення про новий або зміна положення про діючий підрозділ, як правило, приводить до перегляду (коригування, зміни) положень про інші підрозділи;

5) положення у міру зміни функцій підрозділів, методів їх виконання, ролі і місця підрозділу в системі управління необхідно переглядати (як правило, один раз на три роки).

Положення затверджуються керівником підприємства або його заступником відповідно до встановленого між ними розподілу функцій. Підготовку і затвердження положень, тобто введення їх у дію, доцільно здійснювати одночасно для всіх підрозділів або згідно з графіком.

Тимчасові положення розробляються на один рік, після чого їх доопрацьовують, уточнюють, редагують і затверджують як постійні.

Підрозділи, що виконали своє завдання і діяльність яких перестала бути необхідною, слід розформовувати.

Положення про підрозділ, як правило, має такі розділи: загальні положення; функції підрозділу; права; відповідальність підрозділу; відносини з іншими підрозділами.

Посадова інструкція – *організаційно-розпорядчий документ, що регламентує роботу виконавця і визначає його компетенцію; її наявність – необхідна передумова раціональної організації праці*.

Наразі зміст посадової інструкції залежить у першу чергу від обраного підходу до виконання завдання.

Найпоширенішими є три варіанти такого рішення:

I. Зміна й виправлення попередніх документів, використання їх як трафарету.

II. Залучення до складання посадової інструкції співробітників, які будуть її виконувати.

III. Тарифно-кваліфікаційні довідники.

8.2. Система оцінювання роботи працівників з реалізації політики, програм і планів щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства

Для реалізації фінансово-економічної безпеки на підприємстві, організації, установі необхідно застосовувати персонал із відповідною кваліфікацією. Вони повинні бути не тільки професіоналами, здатними нетрадиційно і творчо вирішувати складні завдання діяльності підприємствами, установами, організаціями, всіляко захищати їх інтереси, не допускати правопорушень і злочинних дій. Реалізувати такий підхід можна тільки тоді, коли визначальною фігурою буде працівник.

Необхідно здійснювати перевірку професійних здібностей кандидатів.

За певних умов може з’явитися необхідність у проведенні додаткової, більш

глибокої перевірки. Насамперед, більш ретельно вивчається найближче оточення кандидата: друзі; партнери по спілкуванню, відпочинку, інтересах; сім'я.

Вивчаючи кандидата, слід бути обережним і не допускати порушення його прав.

У ході оцінки кандидатів визначаються: відповідність їх вимогам робочих місць, на які вони претендують; здатність до аналізу виробничих ситуацій і прийняття самостійних рішень; мотиви прагнення зайняти відповідну посаду в банку; їх внутрішня культура, відповідний менталітет; комунікабельність; сприйняття нового, прагнення до навчання (необхідність додаткового навчання); перспективи розвитку і кар'єри.

Для оцінювання роботи працівників з реалізації політики, програм і планів щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства необхідно враховувати показники, які базуються на:

- інформаційно-аналітичному забезпеченні;
- на напрямах забезпечення кадрової політики;
- прийомі, русі та звільнені робітників;
- психологічних аспектах;
- інструментах підбору, збереження та зростання кваліфікації персоналу;
- застосуванні інформаційних безпекових технологій та інструментів;
- формуванні корпоративної етики та репутації;
- інформаційному захисті;
- економічному на фінансовому забезпеченні.

Питання для розгляду:

1. Які структурні підрозділи застосовуються для забезпечення фінансово-економічної безпеки на підприємстві, установі, організації.
2. Охарактеризуйте посадову інструкцію.
3. Які рекомендації використовуються для розробки Положення про підрозділ фінансово-економічної безпеки підприємства, установи, організації.
4. Визначте напрями оцінки роботи працівників з реалізації політики, програм і планів щодо забезпечення фінансово-економічної безпеки установи, організації, підприємства.

Тема 9. Політика економічної безпеки установи, організації, підприємства. Концепція фінансово-економічної безпеки підприємства, установи, організації

9.1. Політика економічної безпеки установи, організації, підприємства.

9.2. Концепція фінансово-економічної безпеки підприємства, установи, організації.

Література: [16, 17, 21, 26, 70, 78].

9.1. Політика економічної безпеки установи, організації, підприємства

Чинники, що формують напрями політики економічної безпеки підприємства, організації установи, різноманітні і в кожній галузі виробництва мають свою специфіку. Однак є загальні, типові чинники, що впливають на політику економічної безпеки:

1. Безпосередні чинники виробництва – основні чинники, які безпосередньо забезпечують діяльність виробництва. До них належать: безпосереднє розміщення підприємства (територія); наявні природні ресурси та умови їх розміщення на цій території, доступність використання та якісні показники; наявність трудових ресурсів, їх освітньо-кваліфікаційний рівень; наявна виробнича інфраструктура, можливий обсяг її використання; соціально-економічна інфраструктура і рівень матеріального достатку населення.

2. Стабільний попит на продукцію – чинник, який також відіграє важливу роль у рівномірному пропозиційному розвитку виробництва. Він охоплює: укладені довготермінові контракти на реалізацію продукції з її споживачами; рівень конкурентоспроможності продукції, що виробляється; якісно-гарантійні показники виробів; обґрунтовані прогнози щодо стабільності ринку певного виду продукції; державне та регіональне замовлення на виготовлену продукцію.

3. Надійність постачальників, передусім тих, що забезпечують постачання основної сировини і матеріалів. Для цього потрібно: мати довготермінові договори на поставку необхідної сировини і матеріалів, враховуючи терміни постачання, та їх якісні показники; знати можливості постачальників і не допускати монопольності в їх поставках, для цього, як правило, потрібно мати 3-4 і більше постачальників сировини та матеріалів, щоб була гарантія стабільної цінової політики щодо сировини, матеріалів та інших комплектуючих.

4. Зовнішня конкуренція на продукцію, призначену на експорт. Ця продукція має: відповідати міжнародним стандартам; за якісними показниками і сервісним обслуговуванням бути конкурентоспроможною; мати обґрунтовану та прогнозовану перспективу; бути конкурентоспроможною щодо продукції, яка імпортується в нашу країну, з метою скорочення ввезення в Україну продукції, яку можуть виготовляти вітчизняні підприємства.

5. Державне економічне регулювання діяльності підприємства, яке полягає: у захисті власного товаровиробника незалежно від форм власності на засоби виробництва; регулюванні державної податкової політики; сприянні виробництву, враховуючи економічні, територіальні та інші аспекти; сприянні виробництву продукції, яка ввозиться як критичний імпорт; державному замовленні на товари, які фінансуються за рахунок бюджету і скорочення імпорту на ці товари.

6. Надійний захист комерційної таємниці. Держава має гарантувати таємницю на науково-технічні досягнення, розроблення нових технологій, інтелектуальну власність, ноу-хау, в тому числі й комерційні таємниці.

7. Компетентність керівництва підприємства. Найважливіші чинники, які можуть найбільш активно впливати на рівень економічної безпеки підприємства, – це високий професіоналізм керівництва і команди його менеджерів (висококваліфіковані кадри; система їх підготовки і форми навчання; створення

для них відповідних виробничих і соціально-економічних умов).

9.2. Концепція фінансово-економічної безпеки підприємства, установи, організації

Концепція фінансово-економічної безпеки підприємства, установи, організації представляє собою систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань захисту законних інтересів і майнових прав суб'єктів господарювання від протиправних дій і недобросовісної конкуренції.

Головним завданням та метою Концепції є побудова системи економічної безпеки суб'єктів господарювання для надійного захисту їх інтересів від зовнішніх і внутрішніх загроз.

Забезпечення економічної безпеки є однією із головних складових успішного ведення господарської діяльності.

Концепція визначає мету та завдання системи економічної безпеки, принципи і правові основи її організації та функціонування, види загроз безпеці суб'єктів господарювання, а також основні складові системи безпеки, включаючи правовий, організаційний та інженерно-технічний захист.

У рамках Концепції визначаються зовнішні загрози, як протиправна діяльність кримінальних структур, конкурентів, юридичних та фізичних осіб, що займаються промисловим шпигунством, рейдерством або шахрайством, неплатоспроможних ділових партнерів, раніше звільнених за різні проступки власних працівників, а також правопорушення з боку корумпованих елементів з числа представників контролюючих, правоохоронних та інших державних органів.

Внутрішні загрози – це діяльність чи бездіяльність (у тому числі навмисна та ненавмисна) окремих посадових осіб суб'єктів господарювання, що суперечить їх майновим правам та інтересам, наслідками яких можуть бути нанесення економічної шкоди суб'єкту господарювання, виток або втрата інформаційних ресурсів (втому числі відомостей, що становлять комерційну таємницю та/або конфіденційну інформацію), підрив їх ділового іміджу, виникнення проблем у взаємостосунках з реальними та потенційними партнерами, конфліктних ситуацій з представниками кримінального середовища, конкурентами, контролюючими та правоохоронними органами, виробничий травматизм або загибель персоналу тощо.

Особливе значення мають ризики як ймовірність втрати цінностей (об'єктів прав власності, фінансових, матеріальних, інформаційних, товарних ресурсів суб'єктів господарювання) в результаті діяльності, якщо обставини та умови проведення діяльності будуть змінюватися у напрямі, який відрізняється від передбаченого планами і розрахунками.

У рамках Концепції визначається стан захищеності як здатності суб'єктів господарювання надійно протистояти будь-яким зовнішнім або внутрішнім загрозам, спробам з боку юридичних чи фізичних осіб завдати шкоди їх законним інтересам.

Правову основу Концепції економічної безпеки складають Конституція

України, Господарський і Цивільний кодекси України, інші нормативно-правові акти.

Правовий захист суб'єктів господарювання, їх майнових прав і інтересів від злочинних зазіхань забезпечується на підставі норм Кримінального і Кримінально-процесуального кодексів, законів України «Про прокуратуру», «Про міліцію», «Про Службу безпеки України», «Про оперативно-розшукову діяльність» та інших.

У рамках Концепції до об'єктів, що підлягають захисту від потенційних загроз та протиправних зазіхань, відносяться:

1. Суб'єкти господарювання, їх працівники.

2. Інформаційні ресурси, що складають комерційну таємницю та конфіденційну інформацію на паперовій, магнітній, іншій основі, інформаційні масиви та бази даних, програмне забезпечення, інформативні фізичні поля різного характеру.

3. Засоби і системи інформатизації (автоматизовані системи і обчислювальні мережі різного рівня та призначення, лінії телефонного, факсимільного, радіозв'язку, технічні засоби передачі та відображення інформації, допоміжні технічні засоби і системи).

4. Власність суб'єктів господарювання (майнові комплекси, будівлі, споруди, машини, устаткування, транспортні засоби, сировина і матеріали, грошові кошти, цінні папери та інше майно виробничого, соціального, культурного призначення, продукти інтелектуальної і творчої діяльності).

У рамках Концепції основними складовими забезпечення безпеки ресурсів є:

- безпека інформаційних ресурсів;
- фізичний захист (безпека) матеріальних об'єктів.

Питання для розгляду:

1. Які чинники впливають на формування політики економічної безпеки установи, організації, підприємства.
2. Охарактеризуйте представлені чинники, які впливають на формування політики економічної безпеки установи, організації, підприємства.
3. Визначте концепцію фінансово-економічної безпеки підприємства, установи, організації.
4. Охарактеризуйте види загроз, які враховуються у рамках концепції фінансово-економічної безпеки підприємства, установи, організації.
5. Визначте об'єктами захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/254.
2. Кодекс України про адміністративні правопорушення [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80731-10/page].
3. Кримінальний Кодекс України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14/page13.
4. Про захист інформації в автоматизованих системах. Закон України № 2594-IV від 31 травня 2005 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2594-15.
5. Про захист від недобросовісної конкуренції. Закон України № 236/96-ВР від 7 червня 1996 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80.
6. Про інвестиційну діяльність. Закон України № 1560-XII від 18 вересня 1991 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1560-12/page2.
7. Про основи національної безпеки України. Закон України № 964-IV від 19 червня 2003 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/964-15.
8. Про підприємства в Україні. Закон України № 887-XII від 27 березня 1991 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/887-12/page2.
9. Про міжнародні договори України. Закон України від 29 червня 2004 року № 1906-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1906-15.
10. Про ратифікацію Європейської конвенції про видачу правопорушників, 1957 рік, Додаткового протоколу 1975 року та Другого додаткового протоколу 1978 року до Конвенції. Закон України (Відомості Верховної Ради (ВВР), 1998, № 23, ст. 129) (Із змінами, внесеними згідно із Законом № 1299-XIV від 15.12.99, ВВР, 2000, № 1, ст. 4) [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/mijbogato.html.
11. Аналіз системи фінансової безпеки підприємства / В. В. Каркавчук // Вісник Львівського національного університету ім. Івана Франка. – Львів : Вид. центр ЛНУ ім. Івана Франка, 2007. – Вип. 38. – С. 90-94. – (Сер. «Економічна»).
12. Артамонова Н. С. Визначення рівня економічної безпеки підприємства задля забезпечення ефективного адміністрування [Електронний ресурс] / Н. С. Артамонова. – Режим доступу : http://www.google.com.ua/url.
13. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) / О. І. Барановський. – Київ : КНТЕУ, 2008. – 759 с.
14. Бендиков М. А. Экономическая безопасность промышленного предприятия в условиях кризисного развития / М. А. Бендиков // Менеджмент в России и за рубежом. – 2000. – № 2. – С. 17-29.
15. Берлач А. І. Безпека бізнесу : навч. посіб. / А. І. Берлач. – Київ : Університет «Україна», 2007. – 280 с.

16. Біломістна І. І. Стратегія забезпечення фінансової безпеки промислових підприємств України [Електронний ресурс] / І. І. Біломістна, Є. І. Грохольська. – Режим доступу : www.nbuv.gov.ua.

17. Бланк И. А. Управление финансовой безопасностью предприятия / И. А. Бланк. – Київ : Ника-центр, Эльг, 2008. – 784 с.

18. Богатирьова Р. В. Про три загрози для безпеки України в 2011 році [Електронний ресурс] / Р. В. Богатирьова. – Режим доступу : http://www.ukrinform.info/bogatirova-ozvuchila-tri.

19. Бурцев В. В. Факторы финансовой безопасности [Электронный ресурс] / В. В. Бурцев // Менеджмент в России и за рубежом. – 2001. – № 1. – Режим доступа : htt://www.dis/ru/libraru/manag/archive/2001/1/933.html.

20. Василенко В. О., Ткаченко Т. І. Стратегічне управління : навч. посібник / В. О. Василенко, Т. І. Ткаченко. – Київ : ЦУЛ, 2003. – 396 с.

21. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія / Т. Г. Васильців. – Львів : Арал, 2008. – 384 с.

22. Ващенко Н. В. Об идентификации / Н. В. Каретникова, Н. В. Ващенко // Методы менеджмента качества. – 2005. – № 6. – С. 52.

23. Вечканов Г. С. Экономическая безопасность : учебник [для студ. ВНЗ] / Г. С. Вечканов. – Санкт-Петербург : Изд-во «Питер», 2007. – 384 с.

24. Вітлінський В. В. Аналіз, моделювання та управління економічним ризиком : навч. посібник / В. В. Вітлінський, П. І. Верченко. – Київ : КНЕУ, 2000. – 292 с.

25. Визначення цілі та завдання інформаційно-аналітичного забезпечення (ІАЗ) [Електронний ресурс]. – Режим доступу : http://pidruchniki.ws/15830523/politologiya/viznachennya_tsili_zavdannya_informatsiyno-analitichnogo_zabezpechennya_iaz#.

26. Герасимчук З. В. Економічна безпека регіону: діагностика та механізм забезпечення : [монографія] / З. В. Герасимчук, Н. С. Вавдіюк. – Луцьк : Надстир'я, 2006. – 244 с.

27. Глазьев С. Ю. Экономическая безопасность / С. Ю. Глазьев // Политическая энциклопедия. В 2 т. Т. 1 А-М / под рук. наук. проекта Г. Ю. Семигина. – Москва : 1999. – 653 с.

28. Глобалізація і безпека розвитку : монографія / за ред. О. Г. Білоруса. – Київ : КНЕУ, 2001. – 733 с.

29. Говорина О. В. Разработка механизма оценки экономической безопасности предприятия в рыночных условиях / О. В. Говорина // Вестник КрасГАУ. – 2008. – № 3. – С. 13-19.

30. Горячева К. С. Механізм управління фінансовою безпекою підприємства : автореф. дис. канд. екон. наук : 08.06.01 [Електронний ресурс] / К. С. Горячева ; Київ. нац. ун-т технологій та дизайну. – Київ, 2006. – 16 с.

31. Горячева К. С. Фінансова безпека підприємства. Сутність та місце в системі економічної безпеки / К. С. Горячева // Економіст. – 2007. – № 8.

32. Гринюк Н. А. Методичні підходи до обґрунтування індикаторів оцінки рівня фінансової безпеки підприємства / Н. А. Гринюк // Проблеми науки. – 2008. – № 6. – С. 35-40.

33. Гринюк Н. А. Управління фінансовою безпекою підприємства в процесі його реструктуризації / Н. А. Гринюк // Проблеми науки. – 2008. – № 9. – С. 19-23.

34. Доценко І. О. Методичні основи оцінки ризиків підприємницької діяльності як складової системи управління економічною безпекою підприємства [Електронний ресурс] / І. О. Доценко. – Режим доступу : www.archive.nbuv.gov.ua/portal/natural.

35. Дєгтяр А. О. Аналітично-організаційне забезпечення прийняття та реалізації державно-управлінських рішень : дис. д-ра наук з держ. управління : 25.00.02 / Донецький держ. ун-т управління. – Донецьк, 2005 – Проект Концепції формування та функціонування інформаційно-аналітичної системи органів державної влади та органів місцевого самоврядування [Електронний ресурс]. – Режим доступу : http://www.kmu.gov.ua.

36. Довбня С. Б. Діагностика рівня економічної безпеки підприємства / С. Б. Довбня, Н. Ю. Гічова // Фінанси України. – 2008. – № 4. – С. 88-97.

37. Донець Л. І. Економічні ризики та методи їх вимірювання : навч. посібник / Л. І. Донець. – Київ : Центр навчальної літератури, 2006. – 312 с.

38. Обгрунтування господарських рішень та оцінювання ризиків : навч. посіб. / за заг. ред. Л. І. Донець. – Київ : ЦУЛ, 2012. – 472 с.

39. Донець Л. І. Економічна безпека підприємства : навч. посібник / Л. І. Донець, Н. В. Ващенко. – Київ : Центр навчальної літератури, 2008. – 240 с.

40. Доронин А. И. Бизнес-разведка [Текст] / А. И. Доронин. – Москва : Ось-89, 2002. – 288 с.

41. Дубецька С. П. Економічна безпека підприємств України / С. П. Дубецька // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України : зб. матер. наук.-практ. конф., 16-17 травня 2001 р. – Київ : Вид-во Європ. ун-ту, 2003. – С. 146-171.

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

43. Єрмошенко М. М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення : [монографія] / М. М. Єрмошенко. – Київ : Київ. нац. торг.-екон. ун-т, 2001. – 209 с.

44. Іванюта Т. М. Економічна безпека підприємства / Т. М. Іванюна, А. О. Заїчковський. – Київ : Центр учбової літератури, 2009. – 256 с.

45. Иванов А. Экономическая безопасность предприятия / А. Иванов, В. Шлыков. – Москва, 1995. – 265 с.

46. Ільяшенко С. М. Составляющие экономической безопасности предприятия и подходы к ее оценке / С. М. Ільяшенко // Актуальні проблеми економіки. – 2003. – № 3 (21). – С. 12-19.

47. Підхомний О. М. Індикатори оцінки рівня фінансової безпеки суб'єктів господарювання / О. М. Підхомний, Л. С. Яструбецька // Економічні науки : зб. наук. праць. – 2007. – Вип. 23. – С. 234-237. – (Сер. «Облік і фінанси»).

48. Камышникова Э. В. Оценка уровня экономической безопасности машиностроительного предприятия / Э. В. Камышникова // Бизнесинформ. – 2009. – № 7. – С. 77-81.

49. Камишнікова О. В. Методика оцінки рівня економічної безпеки металургійного підприємства / О. В. Камишнікова // Актуальні проблеми економіки. – 2009. – № 11 (101). – С. 77-82.

50. Квасницька Р. С. Деякі методичні аспекти формування системи економічної безпеки підприємства / Р. С. Квасницька, І. О. Доценко // Вісник Хмельницького національного університету. – 2009. – № 2, Т. 1. – С. 34-38.

51. Квасницька Р. С. Концептуальні підходи до визначення сутності поняття економічна безпека підприємств / Р. С. Квасницька, І. О. Тернавська // Вісн. Хмельниц. нац. ун-ту. Екон. науки. – 2008. – № 5, Т. 1. – С. 244-247.

52. Квасницька Р. С. Основні підходи до визначення сутності та класифікаційних ознак ризику в підприємницькій діяльності / Р. С. Квасницька, І. О. Тернавська // Вісн. Хмельниц. нац. ун-ту. Екон. науки. – 2008. – № 2, Т. 1. – С. 24-26.

53. Конспект лекцій з дисципліни «Стратегічний аналіз» (для студентів 5 курсу денної форми навчання спеціальності 8.050106 «Облік і аудит») / К. А. Мамонов. – Харків : ХНАМГ, 2005. – 68 с.

54. Кириленко В. І. Інвестиційна складова економічної безпеки [Текст] : монографія / В. І. Кириленко. – Київ : КНЕУ, 2005.

55. Лаврова Ю. В. Механізм забезпечення фінансової безпеки підприємства // Вісник економіки транспорту і промисловості. – 2010. – № 29. – С. 127-130.

56. Лазаренко М. П., Ніколаєнко К. В. Фінансова безпека підприємства та її управління [Електронний ресурс]. – Режим доступу : http://www.rusnauka.com/1_KAND_2010/ Economics/10_57970.doc.htm.

57. Мамонов К. А. Обліково-аналітичне забезпечення стратегічного управління фінансово-економічною безпекою суб'єктів господарювання будівельної галузі та житлово-комунального комплексу України : монографія / Колектив авторів під керівництвом Т. В. Момот. – Харків : Фактор, 2012. – 536 с.

58. Мамонов К. А. Організаційно-економічний механізм управління стейкхолдерами будівельних компаній: сутність, структура й інформаційний захист / К. А. Мамонов // Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики : збірник наукових праць. – Харків : Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» № 2 (14), квітень-червень, 2011. – С. 75-86.

59. Мамонов К. А. Організаційно-економічний механізм управління стейкхолдерами будівельних компаній: розробка, особливості впровадження, інформаційний захист. Комунальне господарство міст : науково-технічний збірник / К. А. Мамонов. – Харків : ХНАМГ, 2011. – Вип. 100.– С. 227-234. – (Серія «Економічні науки»).

60. Мамонов К. А. Стратегічний аналіз : навч. посібник : для студентів галузі знань 0305 «Економіка та підприємництво». Рекомендовано Міністерством освіти і науки України / Т. В. Момот, К. А. Мамонов. – Харків : ХНАМГ, 2011. – 252 с.

61. Методичні вказівки до вивчення дисципліни «Стратегічний аналіз» (для студентів 5 курсу денної форми навчання спец. 8.050106 «Облік і аудит») / уклад. К. А. Мамонов. – Харків : ХНАМГ, 2006. – 60 с.

62. Методичні вказівки до виконання практичних занять і самостійної роботи з дисципліни «Стратегічний аналіз» (для студентів 5 курсу денної форми навчання, спец. 8.050106 «Облік і аудит») / уклад. К. А. Мамонов. – Харків : ХНАМГ, 2005. – 23 с.

63. Минаев Г. А. Безопасность – менеджмент организации, часть 1, 2, 3 (методология, функции, системы) : учебное пособие / Г. А. Минаев. – Москва : ИПБ, 2005.

64. Новак А. М. Алгоритм формирования параметрической структуры корпоративных интересов и оценки уровня финансово-экономической безопасности и информационной защищенности: инновационный подход / Т. В. Момот, А. Н. Новак // Материалы III Международной научно-практической конференции «Инновационные процессы в социально-экономическом развитии». – Бобруйск, 2012. – С. 56-60.

65. Одинцов А. А. Защита предпринимательства (экономическая и информационная безопасность) : учебное пособие / А. А. Одинцов. – Москва : Междунар. отношения, 2003.

66. Олексієнко Б. М. Інформаційно-аналітичне забезпечення оперативно-службової діяльності державної прикордонної служби України [Електронний ресурс] / Б. М. Олексієнко, В. А. Кириленко. – Режим доступу : http://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd.

67. Онищенко С. В. Економічна безпека як підсистема корпоративної безпеки [Електронний ресурс] / С. В. Онищенко, О. І. Савицька. – Режим доступу : http://eprints.kname.edu.ua/22394/1/153162_%D0%9E%D0%BD%D0%B8%D1%89%D0%B5%D0%BD%D0%BA%D0%BE_%D0%A1%D0%92.pdf.

68. Оцінка фінансової безпеки підприємств на основі відокремленої діагностики кризового стану за поточний та минулі періоди [Електронний ресурс]. – Режим доступу : http://www.economy.nayka.com.ua/index.php?operation=1&iid=752.

69. Прыгунов П. Я. Менеджмент безопасности предпринимательства : [учеб. пособие] / А. С. Соснин, П. Я. Прыгунов. – Киев : Изд-во Европ. ун-та, 2002. – 559 с.

70. Управління фінансово-економічною безпекою : навч. посібник / О. А. Кириченко, С. М. Лаптєв, П. Я. Пригунов та ін. ; за ред. В. С. Сідака. – Київ : Дорадо-Друк, 2010. – 480 с.

71. Редченко К. І. Стратегічний аналіз в бізнесі : навчальний посібник / К. І. Редченко. – Вид. 2-ге доповнене. – Львів : «Новий світ», 2000. – 272 с.

72. Стратегічні цілі і моделі ефективної діяльності підприємства : навч. посібник / Н. А. Сіроштан, В. І. Потапов, Н. І. Білявцев та ін. – Харків : ОКО, 1999. – 203 с.

73. Франчук В. І. Корпоративні відносини в системі безпеки акціонерних товариств / В. І. Франчук // Актуальні проблеми економіки : Науковий економічний журнал. – 2009. – № 11. – С. 145-151.

74. Франчук В. І. Теоретичні засади корпоративної безпеки / В. І. Франчук // Актуальні проблеми економіки : Науковий економічний журнал. – 2009. – № 7. –

С. 161-168.

75. Франчук В. І. Теоретична модель системи забезпечення економічної безпеки акціонерних підприємств [Електронний ресурс] / В. І. Франчук // Науковий вісник НЛТУ України. – 2010. − Вип. 20.8. – С. 155-162. – Режим доступу : http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/20_8/155_Franczuk_20_8.pdf.

76. Шарый Л. Д. Безопасность предпринимательской деятельности : учебник / Л. Д. Шарый. – Москва : «ВК», 2005.

77. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект : монографія / С. М. Шкарлет. – Київ : Книжкове вид-во НАУ, 2007. – 436 с.

78. Шкарлет С. М. Формування економічної безпеки підприємств засобами активізації їх інноваційного розвитку [Електронний ресурс] / С. М. Шкарлет. – Рукопис. – Режим доступу : http://avtoreferat.net/content/view/12612/46/.

79. Ярочкин В. И. Корпоративная разведка / В. И. Ярочкин, Я. В. Бузанова. – Москва : «Ось-89», 2005.

80. Ярочкин В. И. Система безопасности фирмы / В. И. Ярочкин. – Москва : Изд-во «Ось-89», 2003. – 352 с.

81. Al-Shaer E. Firewall policy advisor for anomaly discovery and rule editing. In Integrated network management VIII : managing it all : IFIP/IEEE Eighth International Symposium on Integrated Network Management (IM 2003) / E. Al-Shaer, H. Hamed, March 24-28, 2003, Colorado Springs, USA, page 17. Kluwer Academic Pub, 2003. – P. 33-45.

82. Charles C. Zhang, Marianne Winslett and Carl A. Gunter. On the Safety and E±ciency of Firewall Policy Deployment Proc. of IEEE Symposium on Security and Privacy / Charles C. Zhang, May 2007. – P. 24-54.

83. Howard J. D. An Analysis Of Security On The Internet 1989-1995. PhD thesis, Carnegie Mellon University / J. D. Howard, April 1997. – P. 12-34.

84. Wymeersch E. Corporate governance and financial stability [Text] / Eddy Wymeersch / E. Wymeersch // IMF Working Paper Series. – 2008. – WW/08/11. – P. 1-13.

85. Jaeger T. Policy management using access control spaces. ACM Transactions on Informationand System Security (TISSEC) / T. Jaeger, X. Zhang, A. Edwards, 6(3):327-364, 2003. – P. 23-38.

Навчальне видання

МАМОНОВ Костянтин Анатолійович,
ПИРКОВА Ольга Володимирівна

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«СТРАТЕГІЧНИЙ ТА ІННОВАЦІЙНИЙ МЕНЕДЖМЕНТ У СФЕРІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ»

(*для студентів денної і заочної форм навчання освітнього рівня «магістр» спеціальності 073 – Менеджмент. Управління фінансово-економічною безпекою*)

Відповідальний за випуск *М. В. Кадничанський*

За авторською редакцією

Комп'ютерне верстання *Г. О. Павлова*

План 2014, поз. 123 Л

Підп. до друку 18.02.2014 р. Формат 60×84/16
Друк на ризографі Ум. друк. арк. 3,5
Тираж 50 пр. Зам. №

Видавець і виготовлювач:
Харківський національний університет
міського господарства імені О. М. Бекетова,
вул. Революції, 12, Харків, 61002
Електронна адреса: rectorat@kname.edu.ua
Свідоцтво суб'єкта видавничої справи:
ДК № 4064 від 12.05.2011 р.