**Лекція №5**

**Тема. Оперативні методи протидії корпоративним загрозам.**

**Мета:** визначення сучасних інформаційних загроз захищених корпоративних мереж зв’язку, технічну основу яких традиційно становлять комутаційні системи, що реалізовані на виробничо-відомчих АТС, і саме тому вони є однією з основних сфер системи технічного захисту інформації в Україні, а також визначення методів протидії їм.

**План**

1. Модель програмно-керованої АТС відповідно до нормативних документів системи ТЗІ в Україні.

2. Модель цифрової АТС як програмно-апаратного комплексу.

3. Апаратна структура ЦАТС.

4. Заходи інформаційної безпеки корпоративної мережі на експлуатаційному етапі.

**Вступ**

Сьогодні не існує стандартизованих методик аналізу захищеності ІС, тому в конкретних ситуаціях алгоритми дій аудиторів можуть істотно відрізнятися. Система економічної безпеки кожного підприємства є індивідуальною, її повнота і дієвість залежать від чинної в державі законодавчої бази, від обсягу матеріально-технічних і фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості гарантування безпеки бізнесу, а також від досвіду роботи керівників служб безпеки підприємств.

Надійний захист економічної безпеки підприємства можливий лише за комплексного і системного підходу до її організації. Тому в економіці існує таке поняття, як система економічної безпеки підприємства. Ця система забезпечує можливість оцінити перспективи зростання підприємства, розробити тактику і стратегію його розвитку.

Головне завдання системи управління економічною безпекою підприємства - передбачення і випередження можливих загроз, що призводять до кризового стану, а також проведення антикризового управління, яке спрямоване на виведення підприємства з кризового стану; мінімізація зовнішніх і внутрішніх загроз економічному стану суб'єкта підприємництва, зокрема його фінансовим, матеріальним, інформаційним, кадровим ресурсам, на основі розробленого комплексу заходів економіко-правового і організаційного характеру. Слід мати на увазі, що найбільше значення у справі забезпечення економічної безпеки підприємництва мають первинні економіко-правові та організаційні заходи, що забезпечують фундамент, основу системи безпеки, на відміну від вторинних - технічних, фізичних тощо.

У процесі досягнення поставленої мети фірма вирішує конкретні завдання, які об'єднують усі напрями забезпечення безпеки.

Завдання, вирішувані системою гарантування безпеки:

- прогнозування можливих загроз економічній безпеці;

- організація діяльності із запобігання можливим загрозам (превентивні заходи);

- виявлення, аналіз і оцінювання виниклих реальних загроз економічній безпеці;

- ухвалення рішень і організація діяльності з реагування на виниклі загрози;

- постійне вдосконалення системи забезпечення економічної безпеки підприємництва.

Об'єкт і суб'єкт системи забезпечення економічної безпеки підприємництва тісно взаємопов'язані. Об'єктом системи, як зазначалося, виступає стабільний економічний стан суб'єкта підприємницької діяльності в поточний і перспективний періоди. Конкретними ж об'єктами захисту виступають ресурси: фінансові, матеріальні, інформаційні, кадрові. Суб'єкт системи гарантування економічної безпеки підприємництва має складніший характер, оскільки його діяльність зумовлюється не тільки особливостями і характеристиками об'єкта, а й специфічними умовами зовнішнього середовища суб'єкта підприємницької діяльності. Виходячи з цього, можна виділити дві групи суб'єктів, що гарантують економічну безпеку підприємництва: зовнішні і внутрішні.

До зовнішніх суб'єктів належать органи законодавчої, виконавчої і судової влади, покликані гарантувати безпеку всіх без винятку законослухняних учасників підприємницьких відносин, причому діяльність цих органів не можуть контролювати самі підприємці. Ці органи формують законодавчу основу функціонування і захисту підприємницької діяльності в різних її аспектах і забезпечують її виконання.

До внутрішніх суб'єктів належать особи, що безпосередньо здійснюють діяльність із захисту економічної безпеки певного суб'єкта підприємництва. Суб'єктами можуть виступати: працівники власної служби безпеки фірми (підприємства) та запрошені працівники із спеціалізованих фірм, що надають послуги із захисту підприємницької діяльності.

**1. Модель програмно-керованої АТС відповідно до нормативних документів системи ТЗІ в Україні.**

Нормативні документи системи ТЗІ в Україні [1–6], якими визначена методологія створення системи ТЗІ (технічний захист інформації) ЦАТС (цифрова АТС) та оцінки захищеності її інформаційних ресурсів, були впроваджені в 90-х роках минулого століття. Своєю чергою, технології ЦАТС розвивались дуже динамічно, внаслідок чого традиційна АТС перетворилась на комутаційну платформу, на якій формується розгалужений комплекс програмно-апаратних аплікацій і цифрового абонентського сервісу.

До таких рішень, які стали складовими компонентами ЦАТС за цей період, передовсім можна віднести центри обробки викликів (Call Center), системи обробки абонентських голосових, електронних і факсимільних повідомлень, безпровідний абонентський радіодоступ стандарту DECT. Проте цей розвиток технологій ЦАТС поки що не знайшов свого відображення в НД (нормативний документ) СТЗІ (система ТЗІ) в Україні. Якщо розвиток телекомунікаційних і інформаційних технологій йде у напрямі розробки і впровадження інтегрованих рішень, таких, як аплікації комп’ютерно-телефонної інтеграції (CTI – Computer-Telephone Integration), то в НД СТЗІ ці технології є предметом двох самостійних і несумісних напрямків захисту інформації в комп’ютерному і телекомунікаційному обладнанні.

2. Стан нормативної бази системи ТЗІ в Україні безпосередньо впливає на ефективність державної експертизи СТЗІ ЦАТС та її спроможність забезпечити власників захищених корпоративних мереж зв’язку вичерпною інформацією щодо реалізованої в ЦАТС системи ТЗІ й організаційно-технічними заходами з усунення "слабких місць" у ній, особливо за умов використання різноманітних програмно-апаратних аплікацій ЦАТС.

3. Визначення методів і напрямків технічного захисту ЦАТС часто відокремлюється від телекомунікаційних та інформаційних технологій, з якими вони взаємодіють у корпоративних мережах зв‘язку і через які можуть реалізовуватись інформаційні атаки на ЦАТС. 4. Сьогодні в технічній літературі (у відкритій і спеціальній) практично відсутні публікації з викладенням принципів побудови системи ТЗІ ЦАТС, які були б пов’язані з технічною реалізацією апаратно-програмної побудови конкретних моделей ЦАТС.

Це об‘єктивно обґрунтовується тим, що виробники ЦАТС практично не поширюють необхідний для цього деталізований опис компонентів ЦАТС, особливо тих, що безпосередньо формують СТЗІ ЦАТС, і не зацікавлені в оприлюдненні у відкритих джерелах інформації їхньої корпоративної політики безпеки, що реалізується в СТЗІ ЦАТС.

Нормативні документи системи ТЗІ України використовують відносно цифрових АТС термін “програмно-керовані АТС”, роблячи акцент на метод програмного управління, а не на принцип комутації, за яким традиційно класифікують АТС. Згідно із цими документами [1–6] з позиції ТЗІ структура програмно-керованої АТС поділяється на дві порівняно незалежні підсистеми: підсистема керування станцією; підсистема комутації абонентських і з'єднувальних ліній зв'язку (КАЗЛ).

Незалежність даних підсистем керування станцією і КАЗЛ розуміють в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми керування станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, через відсутність механізмів реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ і, навпаки, – на підсистемі КАЗЛ з боку підсистеми керування станцією.

Відносність незалежності вищезгаданих підсистем полягає в тому, що за певних умов (внаслідок помилок або некоректних/зловмисних дій), які були допущені на стадіях життєвого циклу АТС, що передують експлуатаційним (наприклад, при встановленні програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС можливі реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ, і, навпаки, – на підсистемі КАЗЛ з боку підсистеми керування станцією.

Наведена структурна схема програмно-керованої АТС із позицій ТЗІ, і моделі інформаційних загроз, що визначаються на її основі в нормативних документах СТЗІ, неповною мірою відображають відповідно сучасну програмно-апаратну архітектуру ЦАТС та інформаційні загрози, які можуть виникати, а саме:

1. Комутаційна матриця цифрової АТС реалізована у вигляді просторово-часового комутатора, що реалізує багатостанційний доступ з часовим розподілом каналів, який є розгалуженими по всій просторовій структурі АТС. Управління комутацією здійснюється за рахунок центрального керуючого пристрою і механізму розподілу ресурсів шинної структури.

2. Така архітектура не передбачає поділу системи управління і комутації на визначені в НД СТЗІ підсистеми керування станцією і комутації абонентських і з’єднувальних ліній зв’язку.

3. Система управління цифрової АТС з позицій СТЗІ розглядається як двоєдина, – з одного боку, децентралізованою, тому що елементи програмного управління є в усіх апаратних компонентах АТС, і централізованою, з іншого, тому що всі вони керуються єдиною системою управління і комутації, порушення роботи якої призводить до виходу з ладу всієї АТС чи модифікації реалізованих нею функцій.

4. На апаратному і програмному рівнях неможливо здійснити інформаційні атаки на визначену НД СТЗІ підсистему комутації абонентських і з’єднувальних ліній зв’язку від атак на систему керування АТС. Тобто інформаційні атаки не можуть поділятися на атаки підсистеми комутації абонентських і з’єднувальних ліній зв’язку й атаки системи керування.

Наведені в переліку НД СТЗІ моделі інформаційних загроз стосовно підсистеми комутації абонентських і з’єднувальних ліній зв’язку фактично реалізуються за допомогою атак безпосередньо на/через абонентські та з’єднувальні лінії (на ці лінії – з метою зняття інформації з них, через них – з метою впливу на систему управління та комутації ЦАТС).

5. Модель програмно-керованої АТС не деталізує достатньою мірою види з’єднувальних і абонентських ліній, термінальних пристроїв, тоді як, наприклад, інформаційні загрози, що можуть бути реалізовані через цифрові і аналогові з’єднувальні лінії, аналогові і цифрові, зокрема радіо-, термінали, мають різні механізми і є різними за своєю суттю.

6. Нині перелік каналів реалізації інформаційних загроз є набагато різноманітнішим, ніж визначений нормативними документами СТЗІ і містить, наприклад, системи програмно-апаратних аплікацій, безпроводового радіодоступу, засобів ІP-телефонії тощо, які є достатньо небезпечними каналами реалізації інформаційних загроз ЦАТС.

7. Сучасний розвиток телекомунікаційних і інформаційних технологій відбувається у напрямі розробки і впровадження інтегрованих рішень, таких, як аплікації комп‘ютерно-телефонної інтеграції, але в НД СТЗІ ці технології, як і раніше, залишаються предметом двох самостійних і несумісних напрямків захисту інформації відповідно в комп‘ютерному і телекомунікаційному обладнанні.

8. Реалізація інформаційних атак на систему керування і комутації можлива як на доексплуатаційній (технологічній), так і на експлуатаційній стадіях життєвого циклу АТС. Нормативне унеможливлення атак на систему управління і комутації на експлуатаційній стадії може відповідно деформувати модель системи ТЗІ АТС, що реалізується на цій стадії життєвого циклу. Така модель не враховує усіх сучасних програмних й апаратних компонентів ЦАТС і не дає змоги ефективно будувати моделі її інформаційних загроз. [7]

**2. Модель цифрової АТС як програмно-апаратного комплексу.**

Цифрова АТС, що розглядається як програмно-апаратний комплекс на апаратному і програмному рівнях, повинна мати структуру, що наведена на рис. 1 та рис. 2.

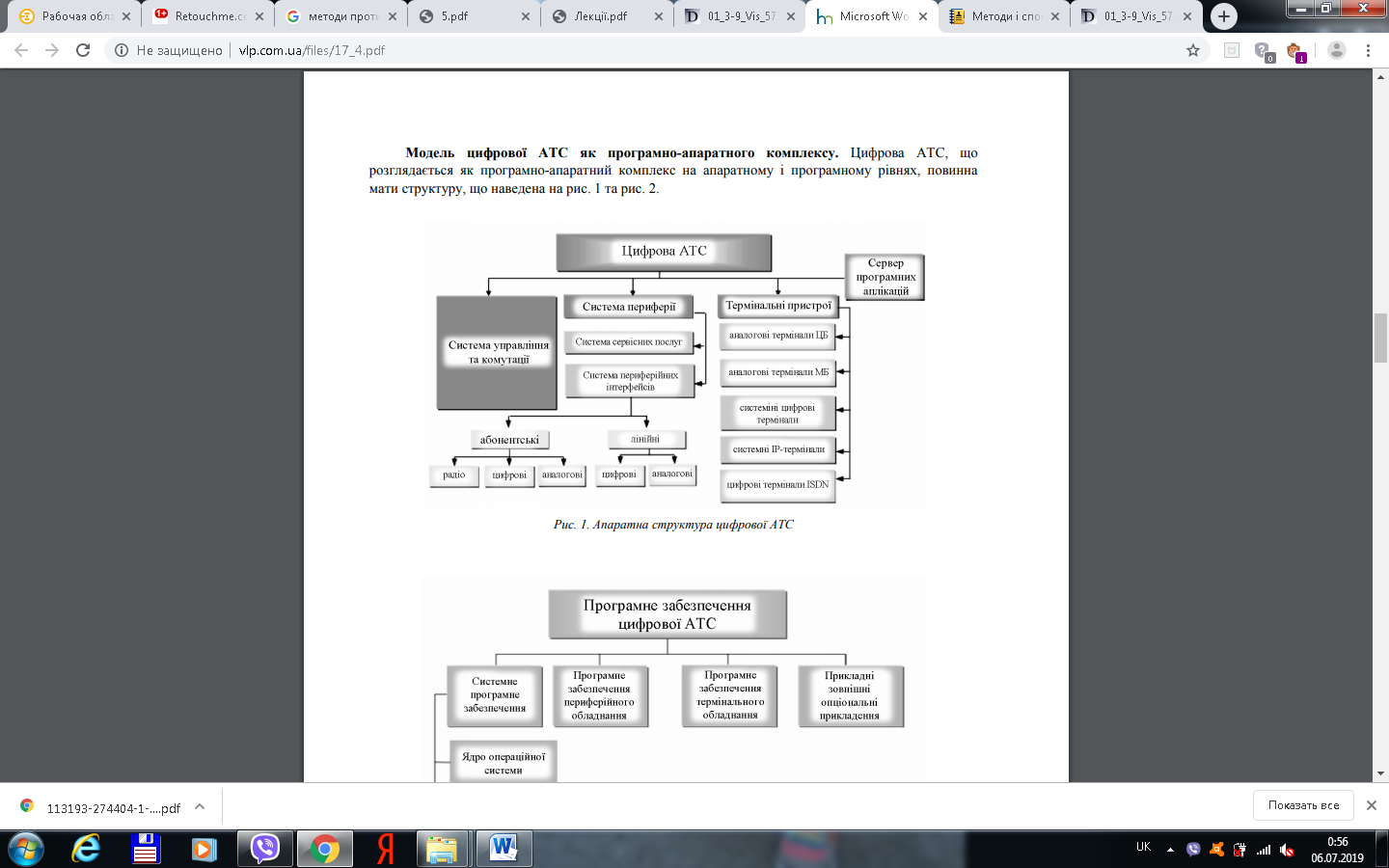


Рис. 1. Апаратна структура цифрової АТС

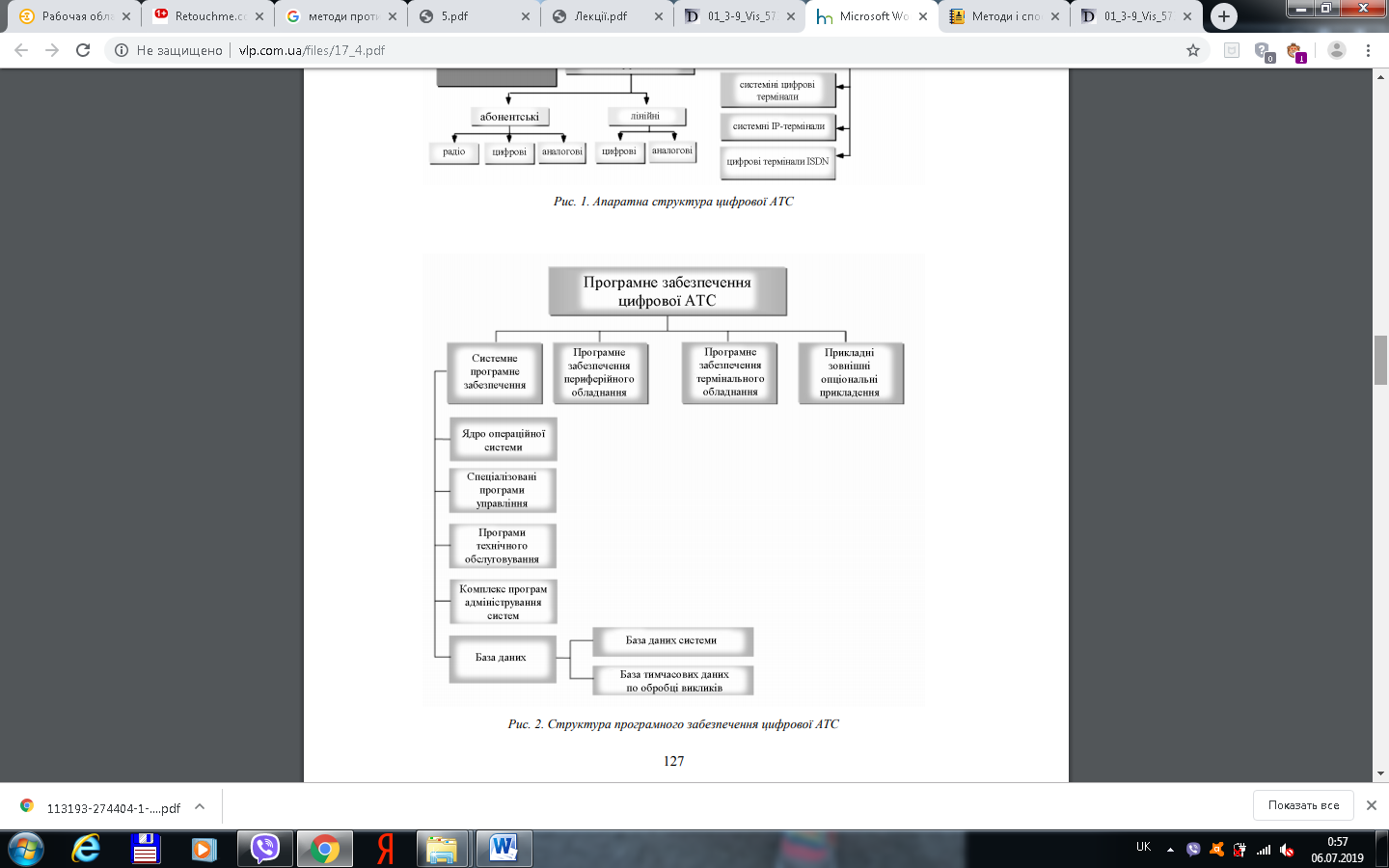


Рис. 2. Структура програмного забезпечення цифрової АТС

**3. Апаратна структура ЦАТС.**

Система управління і комутації становить основу ЦАТС і містить комутатор, центральний керуючий пристрій (центральний процесор), пам’ять і порти вводу-виводу (рис. 3).

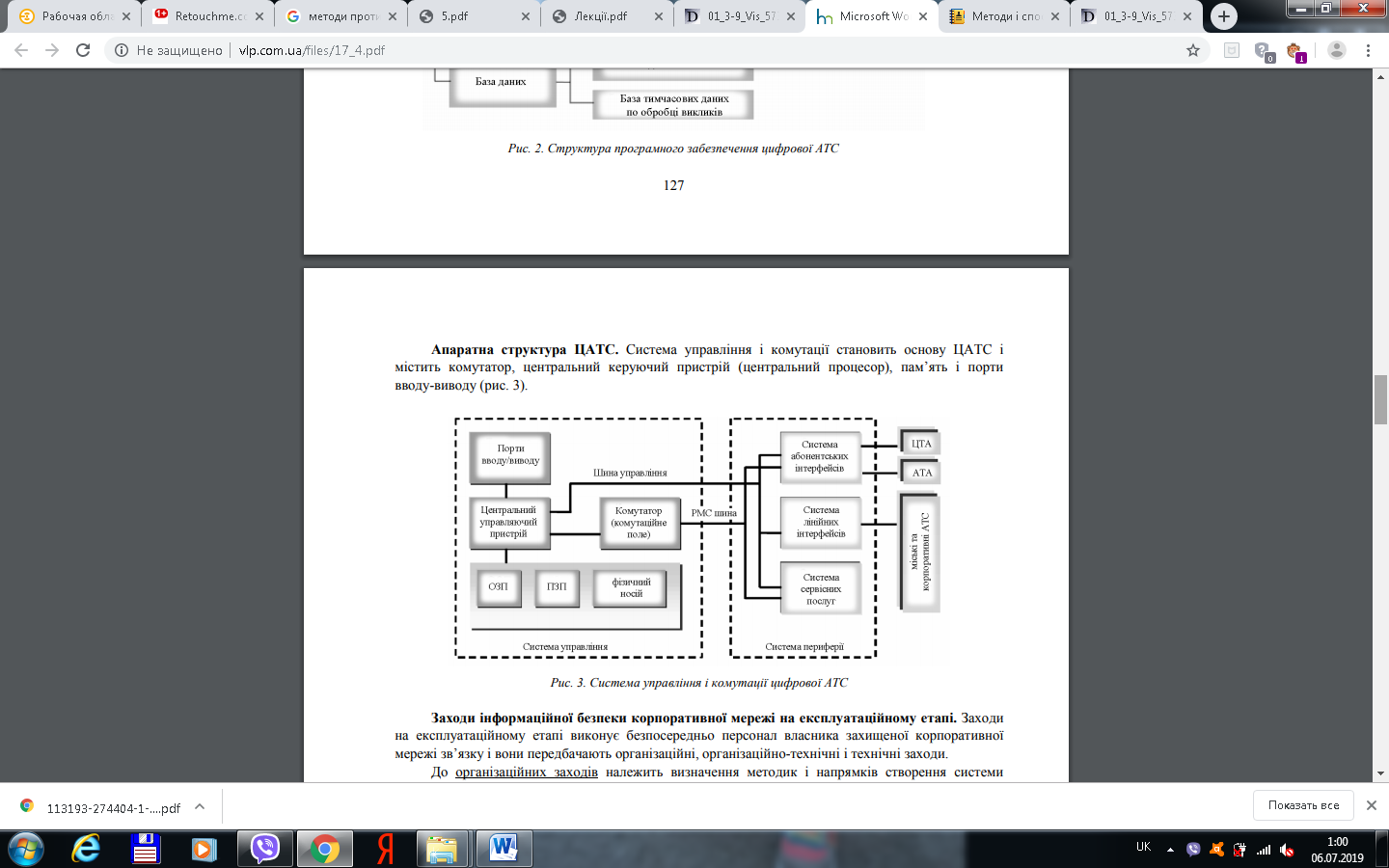


Рис. 3. Система управління і комутації цифрової АТС

**4. Заходи інформаційної безпеки корпоративної мережі на експлуатаційному етапі.**

Заходи на експлуатаційному етапі виконує безпосередньо персонал власника захищеної корпоративної мережі зв’язку і вони передбачають організаційні, організаційно-технічні і технічні заходи.

До організаційних заходів належить визначення методик і напрямків створення системи інформаційної безпеки захищеної корпоративної мережі зв’язку на експлуатаційному етапі, які передбачають відповідну послідовність дій із забезпечення безпеки захищених корпоративних мереж зв‘язку.

В узагальненому вигляді вони можуть бути такими: дослідження мережі зв’язку, розроблення концепції її захисту, вибір методів і обладнання захисту, розроблення методики оцінки ефективності захисту, обґрунтування інвестицій в захист (розрахунок економічного ефекту від заходів, що пропонуються), розробка нормативно-методичних документів, створення центру інформаційної безпеки (центру реагування), створення дослідного (сертифікаційного) полігона, створення фрагмента (дослідної зони) захищеної мережі і здійснення натурних іспитів розроблених методів і апаратури, впровадження системи безпеки мережі поетапно відповідно до концепції за "м’яким" та/або "жорстким" сценарієм.

Крім того, нормативними документами забезпечення інформаційної безпеки захищеної корпоративної мережі визначаються функції безпеки, що реалізуються службами інформаційної безпеки організацій, підприємств і установ, до яких можна зарахувати: аутентифікацію (користувачів, об’єктів і джерел даних); контроль доступу; забезпечення цілісності повідомлень; забезпечення конфіденційності; забезпечення доступності; безвідмовність відправки/доставки; локалізація місця ймовірної атаки; моніторинг і аудит; оповіщення про порушення і відновлення функціонування; адаптації до змінних умов функціонування мережі.

Ці функції планується виконувати за допомогою відповідних механізмів безпеки, в ролі яких можуть бути використані:

- механізми шифрування;

- механізми цифрового підпису;

- механізм обміну інформацією аутентифікації;

- механізми контролю доступу;

- механізми цілісності даних;

- механізм захисту трафіку;

- механізм управління маршрутизацією;

- механізм нотаризації тощо.

До організаційно-технічних заходів належать різноманітні заходи з визначення та встановлення контрольованої зони об’єкта, тобто “території, допуск осіб на яку обмежений та яка знаходиться під контролем” [8].

Визначальним для реалізації контрольованої зони є категорія об’єкта, що присвоюється йому за результатом атестації відповідно до Положення про категоріювання об’єктів ТПКО-95.

Основним критерієм присвоєння категорії об’єкту є найвищий рівень таємності інформації, що обробляється та циркулює на об’єкті. Така контрольована зона може вміщувати декілька концентричних зон, за якими зростають заходи забезпечення інформаційної безпеки відповідно до розміщення компонентів захищеної корпоративної мережі. Зона безпеки захищеної корпоративної мережі зв’язку (рис. 4) передбачає розташування основних засобів технічного обладнання вторинної корпоративної мережі.

Ця зона реалізується як вузол зв’язку з такими елементами: АТС; кросовий зал (крос); лінійно-апаратний зал (з апаратурою каналоутворення); центр електроживлення (у складі блоків живлення та акумуляторних батарей резервного живлення); обладнання технічного захисту інформації (міжмережеві екрани, генератори широкосмугових сигналів тощо); АРМ і ПЕОМ адміністратора захищеної корпоративної мережі; сервер (умовно відокремлений від ПЕОМ адміністратора корпоративної мережі) системи корпоративного аудиту і моніторингу. Організаційно-технічні і технічні заходи з інформаційного захисту корпоративної мережі реалізуються комплексно.

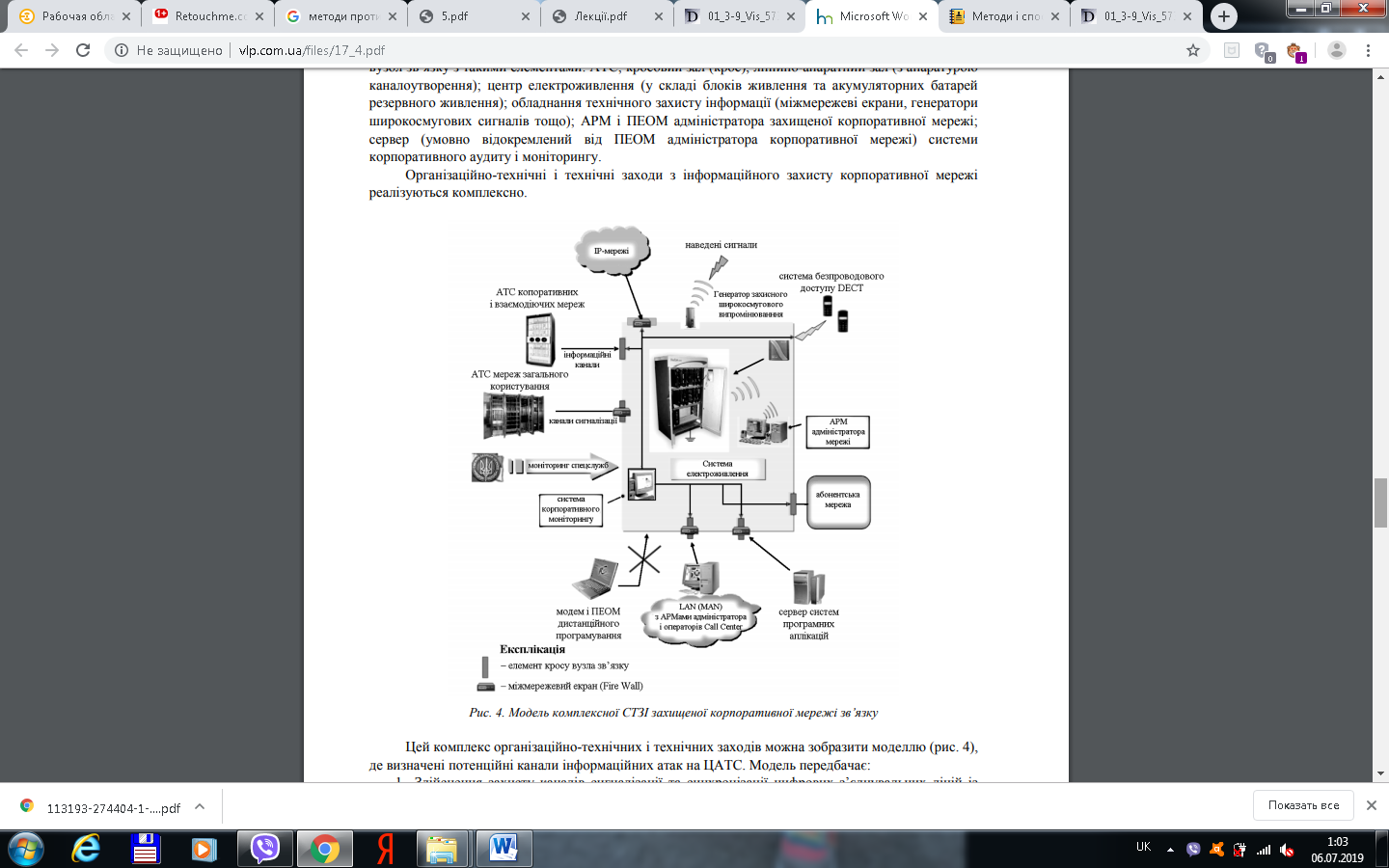


Рис. 4. Модель комплексної СТЗІ захищеної корпоративної мережі зв’язку

Цей комплекс організаційно-технічних і технічних заходів можна зобразити моделлю (рис. 4), де визначені потенційні канали інформаційних атак на ЦАТС.

Модель передбачає:

1. Здійснення захисту каналів сигналізації та синхронізації цифрових з’єднувальних ліній із зустрічними АТС із використанням системи моніторингу та технології міжмережевих екранів.

2. Розміщення ЦАТС і всіх її компонентів у контрольованій зоні (зоні безпеки), де обов’язково реалізуються відповідні організаційно-режимні та обмежувальні заходи.

У приміщенні ЦАТС реалізуються засоби вторинного та резервного електроживлення (під’єднуються в буфері і виконують, крім звичайних, ще й захисні функції). У контрольованих зонах також реалізуються контури захисного заземлення.

3. Використання генераторів шуму для мінімізації загрози використання інформаційних параметрів ПЕМВН для порушення конфіденційності. Отже, можна уникнути загрози використання побічних випромінювань і наведених сигналів від ЦАТС і ЕОМ адміністратора системи.

4. Розміщення базових станцій системи безпровідного доступу стандарту DECT в другій та третій контрольованій зонах (КЗ), що дає змогу забезпечити контроль за їх під’єднанням по провідних каналах через крос до ЦАТС. Однак це не виключає зняття інформації за рахунок випромінювання радіопередавальної частини базових станцій такими засобами, як спеціалізовані сканери та інші аналогічні прилади. Загалом радіус першої КЗ повинен перекривати дальність радіовипромінювання базових станцій.

5. У цій моделі всі інформаційні канали входу в ЦАТС є контрольованими. Канали під’єднання до ЦАТС за протоколом 10/100BaseT сервера систем програмних аплікацій і локальної LAN (MAN) з АРМами адміністратора і операторів Call Center перебувають під моніторингом міжмережевого екрана Firewall. Весь трафік, як внутрішній, так і вхідний/вихідний по з’єднувальних лініях, що на схемі зображений як вхід до контрольованої зони з відповідних напрямків (від зустрічних АТС корпоративної мережі, мереж, що взаємодіють, та мереж загального користування), контролює система корпоративного моніторингу й аудиту.

Такі системи моніторингу з генерацією різноманітних звітних форм (як в екранній, так і в документованій формі) є достатньо дієвим механізмом контролю за трафіком, що передається через ЦАТС.

6. Реалізацію в складі захищеної корпоративної мережі ЦАТС послуг ІР-телефонії (крім мереж державних структур). Захист ІР-шлюзу в ЦАТС забезпечується міжмережевим екраном. Однак заходи інформаційної безпеки не обмежуються лише захистом ІР-шлюзу від ЦАТС до мережі Internet або Ethernet. Захист передбачає використання технологій захищених корпоративних мереж зв’язку, таких, як: міжмережеві екрани, системи виявлення/запобігання атакам, системи аутентифікації, технології віртуальних локальних мереж (VLAN), віртуальних приватних мереж (VPN), шифрування трафіку в режимі “end-to-end”.

Однак все це не дає змоги запобігати інформаційним атакам перехоплення інформаційних пакетів з визначеними параметрами адресата відправлення або отримання за умов використання як транспортної мережі Internet.

7. Захист програмного забезпечення ЦАТС – найвразливіше місце захищеної корпоративної мережі зв’язку [10]:

1) радикальний метод (повна заміна імпортного фірмового ПЗ математичним забезпеченням власної розробки на підставі захищеної операційної системи);

2) консервативний метод (дослідження фірмового ПЗ на предмет недокументованих можливостей (закладок) і їхнє усунення); прагматичний метод (комбінація наведених вище методів – розробка захисної оболонки (shell) для фірмового ПЗ).

Перший метод є найгроміздкішим, але достатньою мірою гарантує стійкість ПЗ при атаках.

Другий метод потребує отримання вихідних текстів від розробника ПЗ.

Останній метод – створення захисної оболонки – є доволі складним. Для його реалізації необхідне розроблення спеціальних апаратно-програмних засобів захисту: конверторів і фільтрів сигналізації, фільтрів програмування АТС, кодерів (шифраторів) Е1, використання технологій віртуальних приватних мереж для напрямлення трафіку управління і сигналізації через спеціально організований тунель. Абонентські мережі у плані технічного захисту інформації є одним із найскладніших компонентів захищеної корпоративної телекомунікаційної мережі, що зумовлено різноманітними факторами. Абонентські мережі в межах території об’єкта (під яким розуміємо офіси установ, відомств, адміністративні і виробничі будівлі підприємств, пункти управління та військові містечка силових та правоохоронних структур тощо) розгортаються відповідно до основного завдання надання послуг зв’язку на робочі місця персоналу.

Це визначає структуру, топологію і ємність абонентських ліній, що прокладаються, зокрема через декілька контрольованих зон, внаслідок чого рівень їхньої безпеки відповідно змінюється [9].

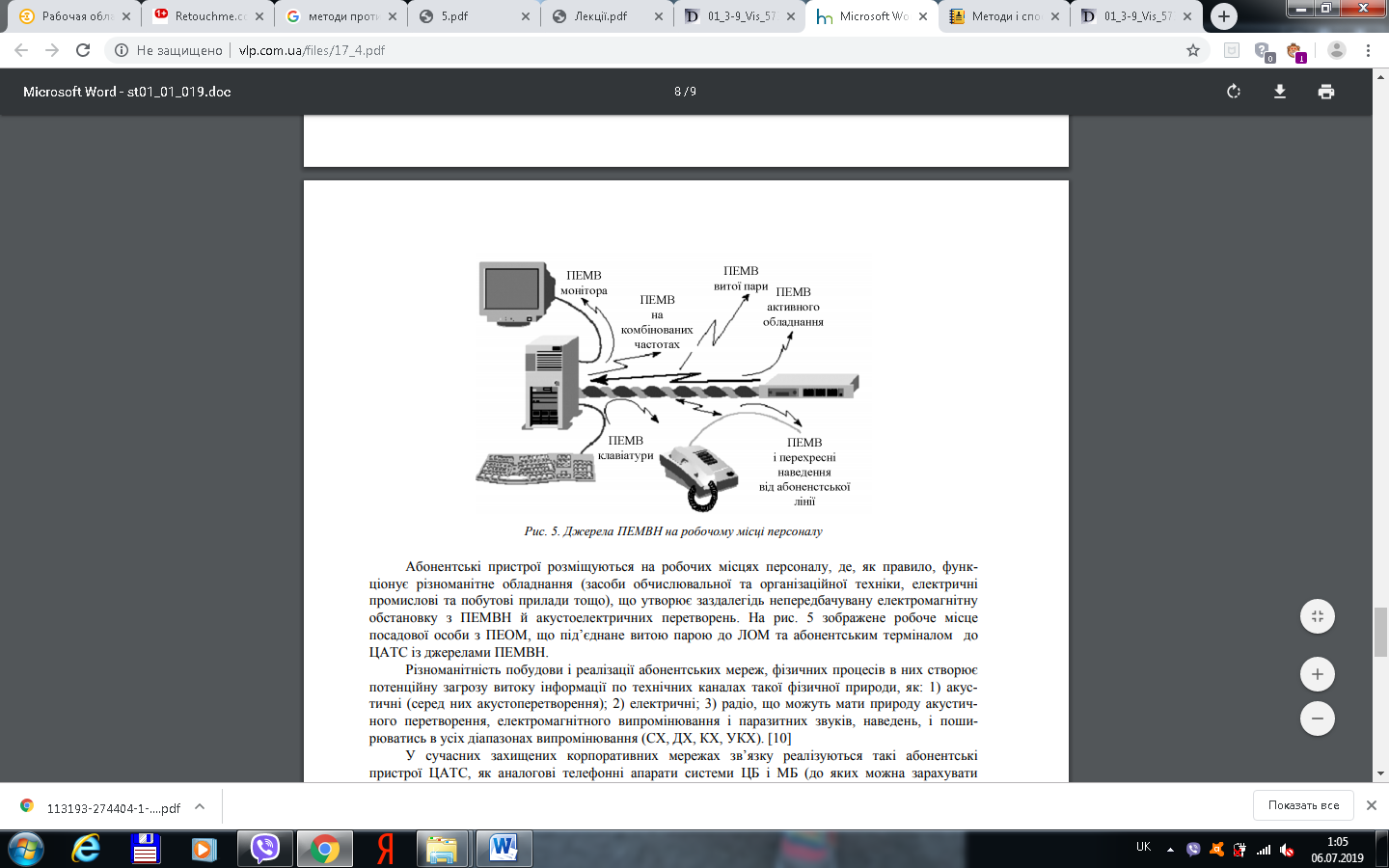


Рис. 5. Джерела ПЕМВН на робочому місці персоналу

Абонентські пристрої розміщуються на робочих місцях персоналу, де, як правило, функціонує різноманітне обладнання (засоби обчислювальної та організаційної техніки, електричні промислові та побутові прилади тощо), що утворює заздалегідь непередбачувану електромагнітну обстановку з ПЕМВН й акустоелектричних перетворень.

На рис. 5 зображене робоче місце посадової особи з ПЕОМ, що під’єднане витою парою до ЛОМ та абонентським терміналом до ЦАТС із джерелами ПЕМВН.

Різноманітність побудови і реалізації абонентських мереж, фізичних процесів в них створює потенційну загрозу витоку інформації по технічних каналах такої фізичної природи, як:

1) акустичні (серед них акустоперетворення);

2) електричні;

3) радіо, що можуть мати природу акустичного перетворення, електромагнітного випромінювання і паразитних звуків, наведень, і поширюватись в усіх діапазонах випромінювання (СХ, ДХ, КХ, УКХ). [10]

У сучасних захищених корпоративних мережах зв’язку реалізуються такі абонентські пристрої ЦАТС, як аналогові телефонні апарати системи ЦБ і МБ (до яких можна зарахувати факсимільні апарати), цифрові системні термінали компаній-виробників, цифрові системи ISDN, цифрові телефонні термінали ІР-телефонії, комп‘ютерні екранні ІР-телефони, цифрові радіотермінали систем безпровідного доступу, а також АРМи систем програмно-апаратних аплікацій і адміністрації мереж зв’язку, що реалізуються на базі ПЕОМ.

При захисті телефонних апаратів і телефонних ліній необхідно враховувати декілька аспектів:

− телефонні апарати (й при покладеній МТ трубці) можуть бути використані для перехоплення акустичної голосової інформації з приміщення, в яких вони встановлені, тобто для підслуховування розмов у цих приміщеннях;

− телефонні лінії, що проходять через приміщення, можуть використовуватись як джерела живлення акустичних закладок, що встановлені в них, а також для передавання перехопленої інформації;

− можливим є перехоплення (підслуховування) телефонних розмов за допомогою гальванічного під’єднання або під’єднання через індукційний давач до телефонної лінії закладок (телефонних ретрансляторів), диктофонів та інших засобів несанкціонованого зняття інформації.

Телефонний апарат має декілька елементів, що здатні перетворювати акустичні коливання на електричні ("мікрофонний ефект").

До них належать дзвінковий ланцюг в аналоговому ТА, телефонний і мікрофонний капсулі. За рахунок електроакустичних перетворень в цих елементах виникають інформаційно небезпечні сигнали. При покладеній мікротелефонній трубці телефонний і мікрофонний капсулі гальванічно від’єднані від телефонної лінії і при під’єднанні до неї спеціальних високочутливих низькочастотних підсилювачів є можливим перехоплення небезпечних сигналів, що виникають в елементах тільки дзвінкового ланцюга. Амплітуда цих сигналів, як правило, не перевищує часток мВ.

При використанні для зняття інформації методу "високочастотного нав’язування", незважаючи на гальванічне від’єднання мікрофона від телефонної лінії, сигнал нав‘язування завдяки високій частоті потрапляє в мікрофонний ланцюг і модулюється за амплітудою інформаційним сигналом.

Отже, в телефонному апараті є необхідним захищати як дзвінкове, так і мікрофонне коло. Для захисту телефонного апарату від витоку акустичної (голосової) інформації по електроакустичному каналу використовуються як пасивні, так і активні методи і засоби [9, 10].

Серед пасивних методів захисту найефективнішими є: обмеження небезпечних сигналів; фільтрація небезпечних сигналів; від’єднання джерел (перетворювачів) небезпечних сигналів.

До основних активних методів належать: подавання під час розмови в телефонну лінію синфазного маскуючого низькочастотного (мовного діапазону) сигналу (метод синфазної низькочастотної маскуючої перешкоди); подавання під час розмови в телефонну лінію високочастотного маскуючого сигналу звукового діапазону (метод високочастотної маскуючої перешкоди); подавання під час розмови в телефонну лінію високочастотного маскуючого ультразвукового сигналу (метод маскуючої ультразвукової перешкоди); підняття напруги в телефонній лінії під час розмови (метод підвищення напруги); подавання під час розмови в лінію напруги, що компенсує постійну складову телефонного сигналу (метод "обнулення"); подавання в лінію при покладеній МТ трубці маскуючого низькочастотного (мовного діапазону) сигналу (метод маскуючої низькочастотної перешкоди); подавання в лінію при прийомі повідомлень маскуючого низькочастотного (мовного діапазону) з відомим спектром (компенсаційний метод); подавання в телефонну лінію високовольтних імпульсів (метод "випалювання").

**Висновок.**

Для покращення управління корпораціями можна запропонувати наступні шляхи та засоби: удосконалення системи захисту прав і законних інтересів акціонерів та забезпечення їх рівноправності; регулярне щоквартальне звітування перед акціонерами про фінансову діяльність товариства; закріплення на законодавчому рівні пропорційного представництва акціонерів у спостережній раді; удосконалення системи розкриття інформації та забезпечення прозорості діяльності товариств; наявність у спостережній раді певної кількості незалежних директорів; введення нового фінансового інструменту на зразок деривативу під назвою «права на акції», який би давав право на участь у вторинній емісії акцій і в торгах на фондовому ринку; розмежування повноважень між органами управління товариства; урахування законних інтересів зацікавлених осіб; публічне визнання акціонерних товариств, які впроваджують найкращу практику корпоративного управління формування та розвиток культури корпоративного управління.

Однак, є низка проблемних питань, пов’язаних з корпоративними конфліктами, що справляють негативний вплив не лише на діяльність корпорацій, а й на ефективність роботи інституційних інвесторів, що виражають інтереси своїх вкладників; з отриманням інсайдерської ренти, що не є специфічно українським явищем, а обумовлена самою специфікою відмінності інтересів власників та менеджменту, а також можливістю менеджерів отримувати дохід від контролю над фінансовими потоками тощо.

Забезпечення інформаційної безпеки держави, всіх її інститутів є актуальним питанням і технічний захист інформації виступає практичним механізмом її реалізації. Робота акцентує увагу на тому, що в реалізації системи ТЗІ цифрових АТС на всіх стадіях життєвого циклу важливими є всі взаємопов’язані і синхронізовані заходи виробників обладнання, державних органів СТЗІ в Україні і власників захищених корпоративних мереж зв’язку. Наявність слабких місць в будь-якій ланці цього єдиного технологічного процесу, як показано в роботі на прикладі об‘єктивного відставання методологій і нормативної бази СТЗІ в Україні від темпів розвитку телекомунікаційних технологій, як і їхня недосконалість, негативно впливають на ефективність комплексного захисту інформаційних і системних ресурсів захищених корпоративних мереж зв’язку.

**Завдання для самостійної роботи**

1. Еволюція поняття «економічна безпека країни».

2. Особливості страхування бізнесу в Україні як основа забезпечення економічної безпеки підприємства.

3. Стратегія і тактика забезпечення економічної безпеки підприє -

мства.

4. Взаємозв’язок категорій «економічна безпека підприємства» та «ризик».

**Питання для самоконтролю**

1. Що являє собою система безпеки?

2. Які методи безпеки включає підрозділ як організована структура?

3. Які заходи безпеки включає підрозділ як організована структура?

4. Які засоби безпеки включає підрозділ як організована структура?

5. Назвіть основні заходи і методи захисту від загроз.

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Guide for Production of Protection Profiles and Security Targets. ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000.

2. Information technology – Security techniques – Protection Profile registration procedures. ISO/IEC 15292: 2000 <http://www.iso.ch/iso/en/commcentre/pdf/Itsecurity0006.pdf>.

3. Куканова Н., Методика оценки риска ГРИФ 2006 из состава Digital Security Office http://www.dsec. ru/about/articles/grif\_ar\_methods/.

4. Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний <http://www.dsec.ru/about/articles/ar_compare/>.

5. Липаев В. В. Анализ и сокращение рисков проектов программных средств http://jetinfo.isib.ru/ 2005/1/2005.1.pdf.

6. Сидак А., Марк К. Mетодология оценки безопасности информационных технологий по общим критериям, <http://jetinfo.isib.ru/2004/6/2004.6.pdf>.

7. Cимонов С. Технологии и инструментарий для управления рисками <http://jetinfo.isib.ru/2003/2/2003.2.pdf>.

8. Тарасов Д.О. Аудит баз даних // Защита информации: Сб. науч. тр. – К.: КМУГА, 2000. – С. 137–143.

10. Гольдштейн Б. С. Мониторинг и предотвращение атак / Б. С. Гольдштейн, И. М. Ехриель, Р. Д. Рерле. – 2006.

**Лекція №6**

**Тема. Об’єкти та суб’єкти корпоративної безпеки.**

**Мета.** Визначити поняття, мету та цілі економічної безпеки підприємства, розкрити її основні складові, об’єкти, суб’єкти та охарактеризувати концепцію управління економічною безпекою підприємства.

**План**

1. Мета та цілі економічної безпеки підприємства.

2. Основні складові економічної безпеки підприємства.

3. Об’єкти, суб’єкти та забезпечення економічної безпеки підприємства.

4. Концепція управління економічною безпекою підприємства.

**Вступ**

Система економічної безпеки включає в себе об'єкти і суб'єкти безпеки, інститути та засоби її забезпечення, функціональну визначеність. Отже, система економічної безпеки підприємства є функціонально визначеною сукупністю об’єктів, суб'єктів, інститутів, механізмів та засобів її забезпечення.

Об'єктами економічної безпеки виступають як економічна система загалом, так і її різні складові: кадрова, фінансова, інформаційна, ресурсне забезпечення.

Суб'єктами економічної безпеки виступають держава та її інститути (міністерства, відомства, біржі, фонди і страхові компанії), а також підприємства, установи й організації як державного, так і приватного сектора економіки.

**1. Мета та цілі економічної безпеки підприємства.**

Економічна безпека на рівні підприємства (фірми) передбачає стійкий розвиток (тобто збалансований і безупинний), що досягається за допомогою використання усіх видів ресурсів і підприємницьких можливостей, за якими гарантується найбільш ефективне їх використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам (загрозам). Її слід розглядати через внутрішній та зовнішній аспект.

Внутрішній аспект полягає у визначенні загрози нанесення підприємством збитку безпеці держави й оцінки рівня збитку (наприклад, підприємства самостійно виходять на зовнішній ринок і здійснюють несанкціоновані дії, що негативно можуть вплинути на імідж усієї держави). Зовнішній аспект полягає в тому, що в Україні умови для економічної безпеки підприємства поки що не створені. Головна мета економічної безпеки підприємства полягає в тому, щоб гарантувати його стабільне та максимально ефективне функціонування зараз і високий потенціал розвитку в майбутньому.

До основних функціональних цілей економічної безпеки підприємств належать:

1) забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності підприємства (організації);

2) забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу того чи іншого суб'єкта господарювання;

3) досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством (організацією);

4) досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу, належної ефективності корпоративних НДДКР;

5) мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

6) якісна правова захищеність усіх аспектів діяльності підприємства (організації);

7) забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації;

8) ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Економічна безпека підприємства характеризується сукупністю якісних і кількісних показників, найважливішим серед яких є рівень економічної безпеки. Рівень економічної безпеки підприємства – це оцінка стану використання корпоративних ресурсів за критеріями рівня економічної безпеки підприємства.

**2. Основні складові економічної безпеки підприємства.**

У рамках підходу до економічної безпеки підприємства як стану, обумовленого впливом зовнішнього середовища, виділяють ресурсно-функціональний підхід. Автори цього підходу розглядають економічну безпеку підприємства як «стан найбільш ефективного використання корпоративних ресурсів для запобігання погроз і забезпечення стабільного функціонування підприємств у даний час і майбутньому». У складі корпоративних ресурсів виділяють, насамперед, ресурси: капіталу, персоналу, інформації, техніки і технології, прав.



Рис. 1. Класифікація суб'єктів забезпечення економічної безпеки підприємств

У зв'язку з цим розрізняють сім функціональних складових економічної безпеки: фінансова, силова, інформаційна, технікотехнологічна, політико-правова, кадрова та інтелектуальна, екологічна.

Основні складові економічної безпеки підприємства:

1) фінансова безпека – розглядає і регулює питання фінансово-економічної заможності підприємства, стійкості до банкрутства. Вона вважається провідною й вирішальною, оскільки за ринкових умов господарювання фінанси є «двигуном» будь-якої економічної системи. Про її стан свідчить рівень рентабельності, частка ринку, доступ до кредитів, ліквідність коштів, курсова вартість цінних паперів, оптимальна структура капіталу тощо;

2) силова безпека – займається режимами, фізичною охороною об'єктів і особистою охороною керівництва, протидією криміналу, взаємодією із правоохоронними й іншими державними органами;

3) інформаційна безпека – заснована не тільки на захисті власної інформації, у тому числі конфіденційної, але й проводить ділову розвідку, інформаційно аналітичну роботу з зовнішніми і внутрішніми суб'єктами тощо.

Належні служби підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки. Вона також передбачає створення системи економічної підтримки прийнятих рішень щодо заходів економічної безпеки;

4) техніко-технологічна безпека – передбачає створення і використання такої технічної бази, устаткування й основних засобів виробництва, таких технологій і бізнес-процесів, що підсилюють конкурентоспроможність підприємства. Про неї свідчить виробничий потенціал підприємства, своєчасність оновлення виробничих фондів, рівень освоєння виробничих потужностей тощо;

5) політико-правова безпека – передбачає всебічне юридичне забезпечення діяльності підприємства, грамотну правову роботу з контрагентами і владою, вирішення інших правових питань;

6) кадрова та інтелектуальна безпека – передбачає запобігання негативним впливам на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому. Належний рівень економічної безпеки у великій мірі залежить від складу кадрів, їхнього інтелекту та професіоналізму, рівня кваліфікації персоналу;

7) екологічна безпека – розглядає проблему охорони екологічної безпеки суспільства від суб'єктів господарювання, що здійснюють виробничо-комерційну діяльність, яку можна вирішити тільки через розробку і ретельне дотримання національних (міжнародних) норм мінімально допустимого вмісту шкідливих речовин, що потрапляють у навколишнє середовище, а також дотримання екологічних параметрів продукції, що виготовляється.

До сфер виробничо-господарської діяльності підприємства, що забезпечують її економічну безпеку, також відносять: ресурсну безпеку (забезпечення виробництва основними видами ресурсів, енергією); соціальну безпеку (рівень заробітної плати, структура доходів працівників, форма власності підприємства); безпеку праці тощо.

Комплексний характер ресурсно-функціонального підходу передбачає дослідження найважливіших факторів, що впливають на стан економічної безпеки підприємства; аналіз розподілу і використання ресурсів підприємства, розгляд економічних індикаторів, що відбивають рівень забезпеченості економічної безпеки і розробку заходів щодо забезпечення максимально високого рівня функціональної складової економічної безпеки підприємства.

Недоліками цього підходу є те, що економічна безпека розглядається загально: і в аспекті ресурсної забезпеченості підприємства, і в аспекті адаптації підприємства до зовнішнього середовища, і в аспекті якості управління – планування, обліку, аналізу тощо.

Тобто економічна безпека ототожнюється із самою діяльністю підприємства та її ефективністю.

Забезпечення економічної безпеки підприємства передбачає регулювання:

− безпеки менеджменту і кадрів – стосується забезпечення фізичної безпеки життя і здоров`я вищого управлінського персоналу і менеджерів середнього та нижчого рівнів, рядових співробітників-виконавців;

− безпеки культури – охоплює взаємини між співробітниками всередині організації, між представниками менеджменту і персоналу, відносини із зовнішніми суб`єктами;

− безпеки інформації і прийняття рішень – полягає в забезпеченні збереження ноу-хау, наукових досліджень і розробок інновацій, обмеженні доступу сторонніх осіб до конфіденційної інформації;

− безпеки виробництва – зводиться до забезпечення захищеності від негативного впливу будівель, споруд, техніки, технології виробництва, виробничих запасів, а також можливостей диверсифікованого виробництва продукції, переорієнтації з одних постачальників на інших, швидкого технічного переозброєння виробництва у випадку переходу на виробництво нової продукції;

− юридичної безпеки – зводиться до збереження наявних і одержаних нових патентів, ліцензій, дозволів; до запобігання або зведення до мінімуму штрафів, пені, інших санкцій і відповідальності за порушення чинного законодавства;

− фінансової безпеки – передбачає якісне бюджетування, зниження податкового пресу, забезпечення надходження необхідного обсягу інвестицій, одержання прибутку, раціональне формування активів і пасивів, дивідендної політики;

− безпеки проведення розвідки – здійснення системи заходів щодо вивчення ситуації на ринках збуту продукції, одержання необхідної інформації про конкурентів, їхні передові дослідження та розробки.

Залежно від ступеня виміру фактори економічної безпеки підприємств поділяють на зовнішні та внутрішні.

До макроекономічних факторів відносять: кризові явища в економіці, стабільність законодавчої бази, інфляційні процеси, рівень безробіття, рівень розвитку фінансової системи, державну політику (промислову, фінансову, соціальну, податкову, кредитну).

Ринкові фактори включають: виробничий і споживчий попит, рівень цін на сировину і готову продукцію, банкрутство контрагентів, платоспроможність конкурентів тощо.

До інших зовнішніх факторів відносять: нестабільну політичну обстановку, темпи НТП, розвиток конкуренції, демографічні тенденції, природні та техногенні фактори.

Внутрішні фактори включають: виробничо-операційні, фінансовоінвестиційні, кадрово-управлінські, маркетингово-комерційні, нормативно-правові. Фактори економічної безпеки підприємства: Зовнішні фактори включають: макроекономічні, ринкові та ін.

До виробничо-операційних факторів відносять такі, як: використання основних і оборотних коштів, структура та ліквідність активів, рентабельність продукції, впровадження нових технологій, структура собівартості, рівень постійних витрат тощо.

Фінансово-інвестиційні фактори включають: нераціональну структуру капіталу, наявність доходних інвестиційних проектів, наявність НДДКР, рівень підприємницького ризику. Кадрово-управлінські фактори – це наявність стратегії розвитку, адекватна ринку система управління, кваліфікація персоналу та його мотивація, організаційна структура управління.

До маркетингово-комерційних факторів належать: цінова політика, планування рекламних заходів, проведення маркетингових досліджень, формування позитивного іміджу тощо.

Нормативно-правові фактори включають: систему контрактів з контрагентами, наявність посадових інструкцій, систему інформаційного забезпечення.

Рівень економічної безпеки залежить від ефективної діяльності служб підприємства, а саме: наскільки вдається запобігати загрозам й усувати збитки від їхніх негативних впливів на різні аспекти функціонування підприємства.

Джерелами таких негативних впливів можуть бути: усвідомлені або неусвідомлені дії людей, організацій, у тому числі органів державної влади, міжнародних організацій або підприємств-конкурентів, а також збіг об`єктивних обставин – стан фінансової кон`юнктури на ринках підприємства, наукові відкриття і технологічні розробки, форс-мажорні обставини тощо.

**3. Об’єкти, суб’єкти та забезпечення економічної безпеки підприємства.**

Виходячи з того, що безпека це форма існування об’єкта (у даному випадку суб’єкта підприємництва) в середовищі небезпек і загроз можемо зазначити, що кінцевий результат безпеки (реалізації її заходів) може співпадати з кінцевим результатом діяльності самого об’єкта.

Звідси метою економічної безпеки суб’єкта підприємництва може бути виключення можливості понесення ним збитків або упущення вигоди, економічне зростання та стабільність.

Головне завдання суб’єктів забезпечення економічної безпеки підприємства – передбачення і випередження можливих загроз, що призводять до кризового стану, а також проведення антикризового управління, яке спрямоване на виведення підприємства з кризового стану; мінімізація зовнішніх і внутрішніх загроз економічному стану суб'єкта підприємництва, зокрема його фінансовим, матеріальним, інформаційним, кадровим ресурсам, на основі розробленого комплексу заходів економіко-правового і організаційного характеру. Слід мати на увазі, що найбільше значення у справі забезпечення економічної безпеки підприємництва мають первинні економіко-правові та організаційні заходи, що забезпечують фундамент, основу системи безпеки, на відміну від вторинних - технічних, фізичних тощо.

Суб'єкт системи гарантування економічної безпеки підприємництва має складніший характер, оскільки його діяльність зумовлюється не тільки особливостями і характеристиками об'єкта, а й специфічними умовами зовнішнього середовища суб'єкта підприємницької діяльності. Виходячи з цього, можна виділити дві групи суб'єктів, що гарантують економічну безпеку підприємництва: зовнішні і внутрішні.

До зовнішніх суб'єктів належать зовнішні органи (законодавчої, виконавчої і судової влади, покликані гарантувати безпеку всіх без винятку законослухняних учасників підприємницьких відносин) та організації, які функціонують самостійно і не підпорядковуються керівництву підприємства, але при цьому їх діяльність істотно впливає на безпеку підприємства.

До внутрішніх суб'єктів належать особи, підрозділи, що займаються цією діяльністю безпосередньо на підприємстві і підпорядковані його керівництву. Їх основним призначенням є постійна діяльність із забезпечення безпеки підприємства. До цієї категорії можна віднести підрозділи, частина функцій у яких полягає в забезпеченні безпеки підприємства (маркетингова служба, юридичний підрозділ тощо). Також персонал та підрозділи підприємства, які в межах своїх посадових інструкцій та положень про підрозділи зобов'язані вживати заходів щодо забезпечення безпеки підприємства.

Залежно від форми власності та підпорядкування суб’єктами забезпечення безпеки можуть виступати державні та недержавні органи. Державні органи – здійснюють повноваження щодо безпеки суб'єктів фінансово-господарської діяльності, до структури яких вони входять, або ж надають послуги стороннім фірмам на умовах укладених договорів, прикладом чого є діяльність Державної служби охорони МВС України щодо заходів безпеки усіх без винятку комерційних банків в Україні. Недержавні органи, які представлені охоронними організаціями, аналітичними центрами, інформаційними та консалтинговими службами, які за відповідну плату на умовах договору надають послуги щодо охорони об'єктів, здійснюють захист інформації, комерційної таємниці тощо. До цієї групи суб'єкті належать і власні служби безпеки підприємства недержавної форми власності.

Суб’єкти забезпечення економічної безпеки можуть класифікуватись в залежності від правової основи функціонування. До офіційних належать органи та організації, що функціонують у межах чинного законодавства України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. До неофіційних організацій належать нелегітимні структури, діяльність яких відбувається поза правовим полем України. Наразі їх функціонування має динаміку до зменшення, що викликано відмовою суб'єктів бізнесу від їхніх "послуг", однак відкидати їх існування не варто. Зазначені суб'єкти, іншими словами "дах", пропонують свої послуги через погрози, насилля, погроми гарантуючи при цьому захищеність від подібних структур. Зазвичай такі послуги пропонуються суб'єктам бізнесу, діяльність яких повністю або частково відбувається в тіні, що є підставою до шантажу.

Організації, що займаються забезпеченням економічної безпеки можуть бути класифіковані залежно від регламенту відносин. Відтак вони можуть регулюватись договором. В основному це стосується зовнішніх організацій, або окремих спеціалізованих фахівців залучених з метою забезпечення безпеки на підприємстві. В іншому випадку порядок взаємодії може регулюватись наказом. Ця форма відноситься до внутрішніх підрозділів. Посадові інструкції, в свою чергу, регулюють діяльність окремих працівників.

Залежно від напряму забезпечення безпеки підприємства суб’єкти можуть класифікувати за визначенням сфер, у яких діють чинники небезпек і загроз. До таких сфер належать: силова безпека, пожежна, інформаційна, кадрова, майнова, економічна, екологічна, технологічна.

Надійність і ефективність системи безпеки підприємства визначають за одним критерієм - відсутністю чи наявністю завданих йому матеріальних збитків і моральної шкоди. Зміст цього критерію характеризується такими показниками:

а) запобігання витоку конфіденційних відомостей;

б) запобігання протиправним діям з боку персоналу підприємства, його відвідувачів, клієнтів або припинення таких дій;

в) збереження майна й інтелектуальної власності підприємства;

г) запобігання надзвичайним ситуаціям;

д) припинення насильницьких злочинів щодо окремих (спеціально виділених) працівників підприємства і груп їх;

е) своєчасне виявлення і припинення спроб несанкціонованого проникнення на об'єкти підприємства, що охороняються.

Політика безпеки підприємства - це орієнтири для дій і ухвалення рішень, які полегшують досягнення цілей. Для встановлення цих загальних орієнтирів необхідно сформулювати цілі забезпечення безпеки підприємства.

Цілі політики безпеки:

- захист фінансових ресурсів підприємства;

- захист прав та інтересів підприємства;

- зміцнення інтелектуального потенціалу підприємства;

- збереження і примноження власності;

- підвищення конкурентоспроможності продукції;

- інформаційне забезпечення діяльності підприємства і підвищення його ефективності;

- орієнтація на стандарти й лідерство;

- сприяння управлінським структурам у досягненні цілей підприємства;

- запобігання залежності від випадкових і недобросовісних ділових партнерів.

З урахуванням викладеного вище можна визначити такі загальні орієнтири дій і ухвалення рішень, які полегшують досягнення цих цілей:

а) збереження і нарощування ресурсного потенціалу;

б) проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності й персоналу підприємства;

в) залучення до діяльності із забезпечення безпеки підприємства всіх його працівників;

г) професіоналізм і спеціалізація персоналу підприємства;

д) пріоритетність несилових методів запобігання загрозам і їх нейтралізації;

е) створення служби економічної безпеки на підприємстві.

Відтак, в залежності від напрямів забезпечення безпеки підприємства можна зробити висновок, що певні організації або підрозділи можуть впливати на ту чи іншу складову (табл. 1).

У цьому контексті систему безпеки можна охарактеризувати комплексом страхових, правових, економічних, охоронних, режимних, пожежних та інших заходів із захисту бізнесу від незаконних посягань, мінімізації або уникнення матеріальних та інших втрат.

Зазвичай увесь комплекс діяльності із забезпечення економічної безпеки покладається на службу безпеки підприємства (у разі її наявності на підприємстві) як основну ланку системи економічної безпеки.

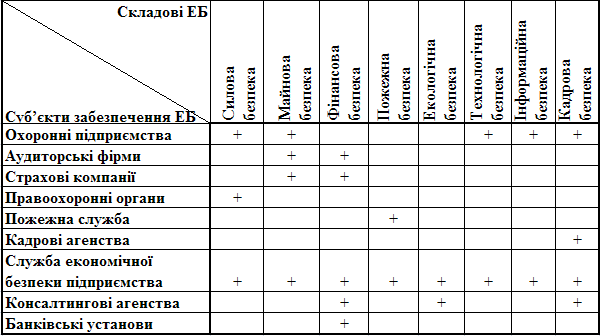
Формування системи економічної безпеки та створення її суб’єктів залежать від розмірів підприємства та його можливостей. Як правило, підприємства малого бізнесу користуються послугами зовнішніх спеціалізованих приватних підприємств (консалтингових, охоронних, страхових тощо). Підприємства середнього бізнесу можуть користуватися комбінованою системою економічної безпеки, спираючись на можливості і ресурси власних підрозділів безпеки та, в міру необхідності, залучаючи зовнішні організації. Великим підприємствам доцільно створювати повноцінну систему економічної безпеки з власною службою та потужними ресурсами.

Об’єктами економічної безпеки суб’єкта підприємництва виступають: фінансові та матеріальні ресурси, технології виробництва, комерційна діяльність, процес управління діяльністю суб’єкта. Відповідно у структурі економічної безпеки можна виділити наступні елементи.

Суб’єктами економічної безпеки за таких умов будуть виступати власники суб’єктів підприємництва, органи управління їх діяльністю та персонал.

Таблиця 1.

Вплив суб’єктів на забезпечення безпеки підприємства

****

Разом з тим, серед видів забезпечення економічної безпеки суб’єктів підприємництва виступають правове, інформаційне, науково-технічне та кадрове.

Правове забезпечення економічної безпеки виконує функцію регулювання взаємовідносин суб’єктів підприємництва як поміж собою, з державою, іншими організаціями, які виникають у них у процесі захисту їх підприємницької, господарської, виробничої, фінансової та інших видів діяльності.

Основу правового забезпечення суб’єкта підприємництва складають правові акти: Конституція та закони України, підзаконні акти органів виконавчої влади, нормативно-правові документи самих суб’єктів та інші документи, які стосуються їх діяльності.

Інформаційне забезпечення спрямоване на формування у керівництва та працівників суб’єктів господарювання знань про ситуацію на ринку, політичну та соціальну ситуацію в певному регіоні чи в країні, особливості небезпек і загроз діяльності суб’єктів підприємництва, основні тенденції розвитку конкретних галузей економіки та підприємництва взагалі і т. і. Для ефективного інформаційного забезпечення підприємства, банки формують власний інформаційний ресурс і використовують загальнодоступні державні інформаційні ресурси та ресурси певних організацій і установ, ведуть пошук необхідної інформації в глобальній інформаційній мережі та інших відкритих джерелах.

Наукове забезпечення економічної безпеки суб’єктів підприємництва пов’язане перш за все з розробкою нових технологій захисту їх інтересів, узагальненням досвіду забезпечення безпеки у сфері економічних взаємовідносин, а також дослідження тенденцій та перспектив розвитку заходів економічної безпеки. Кадрове забезпечення спрямоване на формування у суб’єктів підприємництва надійних, лояльних, стійких до небезпек і загроз, які можуть виникати у підприємницькій діяльності працівників.

Формування такого персоналу може бути здійснено шляхом відбору персоналу, контролю його роботи і поведінки, забезпечення потреб і інтересів працівників, виховання фірмового патріотизму.

Забезпечення економічної безпеки у діяльності суб’єктів підприємництва здійснюється через формування відповідних режимів, зокрема: режиму формування та використання їх ресурсів, режиму поведінки персоналу в різних умовах виробничої діяльності, режиму функціонування інформації, особливого режиму діяльності суб’єктів підприємництва в умовах дії несприятливих факторів економічної, політичної, соціальної ситуації в країні.

Крім того, система економічної безпеки суб’єктів підприємництва забезпечує відповідні режими поведінки самих суб’єктів на ринку з урахуванням змін на ньому та в країні. Тут можуть запроваджуватися такі режими: режим економії, режим активізації, режим виживання і т. д. Формування вказаних режимів забезпечується через участь усіх структур суб’єктів підприємництва у виконанні заходів безпеки по різних напрямках: фінансовому, інформаційному, кадровому, безпеки матеріальних ресурсів, що в свою чергу забезпечить оперативність та своєчасність реагування суб’єктів на будь-які зміни внутрішньої та зовнішньої ситуації.

**4. Концепція управління економічною безпекою підприємства.**

Концепція управління економічною безпекою підприємства – це система теоретико-методологічних поглядів, яка відображає розуміння і трактовку економічної безпеки підприємства та визначає цілі, завдання, методи, принципи, концептуальні моделі та положення управління нею.

Ефективне управління економічною безпекою підприємства повинне базуватись на таких основних принципах:

1. Принцип законності – уся діяльність підприємства повинна носити законний характер, інакше є суттєва загроза закриття такого підприємства відповідними органами як неправомірного. Вся система економічної безпеки та її функціонування мають бути побудовані у відповідності до існуючих в країні правових норм та власних правових актів суб’єктів підприємництва.

2. Принцип економічної доцільності – слід організовувати захист тільки тих об'єктів, витрати на захист яких менше, ніж втрати від реалізації загроз за цими 9 об'єктами. Вартість заходів економічної безпеки не повинна перевищувати вартості отриманих від них економічних результатів.

3. Поєднання превентивних та реактивних заходів економічної безпеки. Превентивними вважаються заходи попереджувального характеру, що дозволяють не допустити виникнення або реалізацію загроз економічній безпеці. Реактивні – це заходи, які приймаються в разі реального виникнення загроз або необхідності мінімізації їх негативних наслідків.

4. Принцип безперервності – функціонування системи забезпечення економічної безпеки підприємництва має здійснюватися постійно.

5. Принцип диференційованості – вибір заходів з подолання загроз, що виникають, відбувається залежно від характеру загрози і ступеня тяжкості наслідків її реалізації.

6. Принцип координації – для досягнення поставлених завдань необхідно постійне узгодження діяльності різних підрозділів служби безпеки, самого підприємства і поєднання організаційних, економіко-правових та інших способів захисту.

7. Повна підконтрольність системи забезпечення економічної безпеки керівництву суб'єкта підприємницької діяльності. Інтереси системи забезпечення економічної безпеки повинні бути підпорядковані загальним інтересам всього підприємства.

8. Принцип цілеспрямованості вказує на те, що всі заходи економічної безпеки мають базуватись на інтересах суб’єктів підприємництва і спрямовуватись на захист тих видів діяльності, які в даний час виконує суб’єкт підприємництва.

9. Контроль як принцип економічної безпеки має забезпечити відповідність отриманих від проведених заходів безпеки результатів тим показникам, які передбачались при їх плануванні, а диверсифікація у свою чергу вимагає з одного боку комплексного підходу при запровадженні заходів безпеки, а з іншого – поширення їх на всі види діяльності суб’єкта підприємництва та всі регіони, в яких реалізуються його інтереси.

10. Баланс інтересів вимагає, щоб забезпечення економічної безпеки здійснювалось з врахуванням інтересів безпеки всіх осіб, які мають справу з тим чи іншим суб’єктом підприємництва: працівники, акціонери, клієнти (споживачі), контрагенти, партнери, держава.

Концептуальні положення управління економічною безпекою підприємства:

1. Моніторинг та діагностику економічної безпеки підприємства необхідно проводити постійно.

2. Економічну безпеку підприємства необхідно досліджувати в статичному та динамічному аспекті.

3. Управління економічною безпекою підприємства повинне бути ключовою складовою стратегічного управління підприємства.

4. Повинно постійно здійснюватись удосконалення захисту інформації підприємства.

5. Повинен здійснюватись контроль доступу сторонніх осіб на територію підприємства.

6. Необхідно ретельно перевіряти контрагентів на предмет їх репутації та порядності ведення бізнесу.

7. Періодично необхідно здійснювати перевірки персоналу підприємства на предмет ймовірності розкриття комерційних таємниць підприємствам-конкурентам.

8. Необхідно знижувати ризики від озброєних пограбувань підприємства.

9. Оцінювально-аналітична система повинна стати центральною частиною управління економічною безпекою підприємства.

10. При оцінюванні рівня економічної безпеки підприємства необхідно враховувати не лише результати діяльності підприємства на поточну дату, а й потенціал, тобто здібності підприємства до забезпечення економічної безпеки підприємства в майбутньому.

11. При оцінюванні рівня економічної безпеки підприємства необхідно використовувати декілька альтернативних методичних підходів.

12. Оцінка значущості функціональних складових економічної безпеки підприємства повинна проводитись за допомогою добре перевірених евристичних методів.

13. Оцінка та аналіз економічної безпеки підприємства повинні базуватись на врахуванні технологічних особливостей підприємства.

14. Оцінювальні показники економічної безпеки підприємства повинні бути скориговані на коефіцієнт значущості стадії життєвого циклу підприємства.

15. Оцінювальні показники економічної безпеки підприємства повинні бути скориговані на коефіцієнт значущості ринкової стратегії підприємства.

16. Управління економічною безпекою підприємства необхідно здійснювати не лише за результатами, а й за потенціалом підприємства.

17. Працівники служби економічної безпеки підприємства повинні володіти навичками побудови економіко-математичних моделей, володіти найсучаснішими пакетами прикладних програм, знати основні підходи до оцінювання рівня економічної безпеки підприємства.

18. Працівники служби економічної безпеки підприємства повинні оперативно реагувати на зміни в зовнішньому середовищі.

**Висновок.** Отже, для забезпечення власної безпеки підприємство має такі засоби: технічні (охороно-пожежні системи, відеоапаратура тощо); організаційні (створення спеціалізованих підрозділів чи структур, які забезпечуватимуть безпеку підприємства, а також система управління); інформаційні (комп'ютери, захисні мережі і сама інформаційна продукція, у т.ч. необхідна для прийняття рішень інформація); фінансові, без яких і функціонування системи безпеки буде неможливим; правові (у т. ч. розробка локальних правових актів з питань функціонування системи управління та забезпечення безпеки); кадрові (передусім, достатня кількість персоналу, який займається питанням безпеки, його професіоналізм); інтелектуальні (залучення висококласних спеціалістів і науковців дозволяє запроваджувати нові системи безпеки). Варто зазначити, що ці засоби потребують комплексного поетапного застосування, а не одночасного запровадження. Активація підприємством вищенаведених засобів у забезпеченні безпеки переводить їх у категорію методів, тобто способів дії. Таким чином, підприємство може застосовувати технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи.

**Завдання для самостійної роботи**

1. Наведіть відмінності між службою безпеки підприємства та службою його економічної безпеки.

2. Виділіть основні відмінності між показниками та індикаторами економічної безпеки підприємства.

3. Основні відмінності при використанні методів експертного оцінювання та економіко-математичних методів при проведенні оцінки рівня економічної безпеки підприємства.

4. Які методи оцінки економічної безпеки необхідно використовувати на макро-, мезо- та мікро- рівнях економіки?

**Питання для самоконтролю**

1. Мета та цілі економічної безпеки підприємства.

2. Основні складові економічної безпеки підприємства.

3. Об’єкти, суб’єкти та забезпечення економічної безпеки підприємства. 4. Концепція управління економічною безпекою підприємства.

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури.**

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

2. Жихор О. Б. Економічна безпека: Навчальний посібник. / О. Б. Жихор, Т. М. Куценко. – Харків: ХІБС УБС НБУ, 2013. – 144 с.

3. Зубок М. І. Економічна безпека суб’єктів підприємництва: навчальний посібник. / М. І. Зубко та ін. – К. : Знання, 2012 – 226 с.

4. Іванюта Т. М. Економічна безпека підприємства: навч. посібник / Т. М. Іванюта, А. О. Заїчковський – К. : Центр учбової літератури, 2009. – 256 с.

5. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства: навч. посібник. / П. І. Мойсеєнко, О. М. Марченко. – Львів, 2011. – 380 с.

6. Отенко І. П. Економічна безпека підприємства : навчальний посібник / укл. І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Х. : Вид. ХНЕУ, 2012. – 356 с.

7. Пилипенко А. А. Організація обліково-аналітичного забезпечення стратегічного розвитку підприємства. Наукове видання. / А. А. Пилипенко. – Харків : Вид. ХНЕУ, 2007. – 276 с.

**Лекція №7**

**Тема. Забезпечення безпеки компанії на внутрішніх та зовнішніх ринках.**

**Мета:** визначення сутності PEST-аналізу, оцінювання факторів впливу внутрішнього та зовнішнього середовища

**План**

1. Діагностика зовнішнього середовища непрямого впливу

2. Діагностика зовнішнього середовища безпосереднього впливу

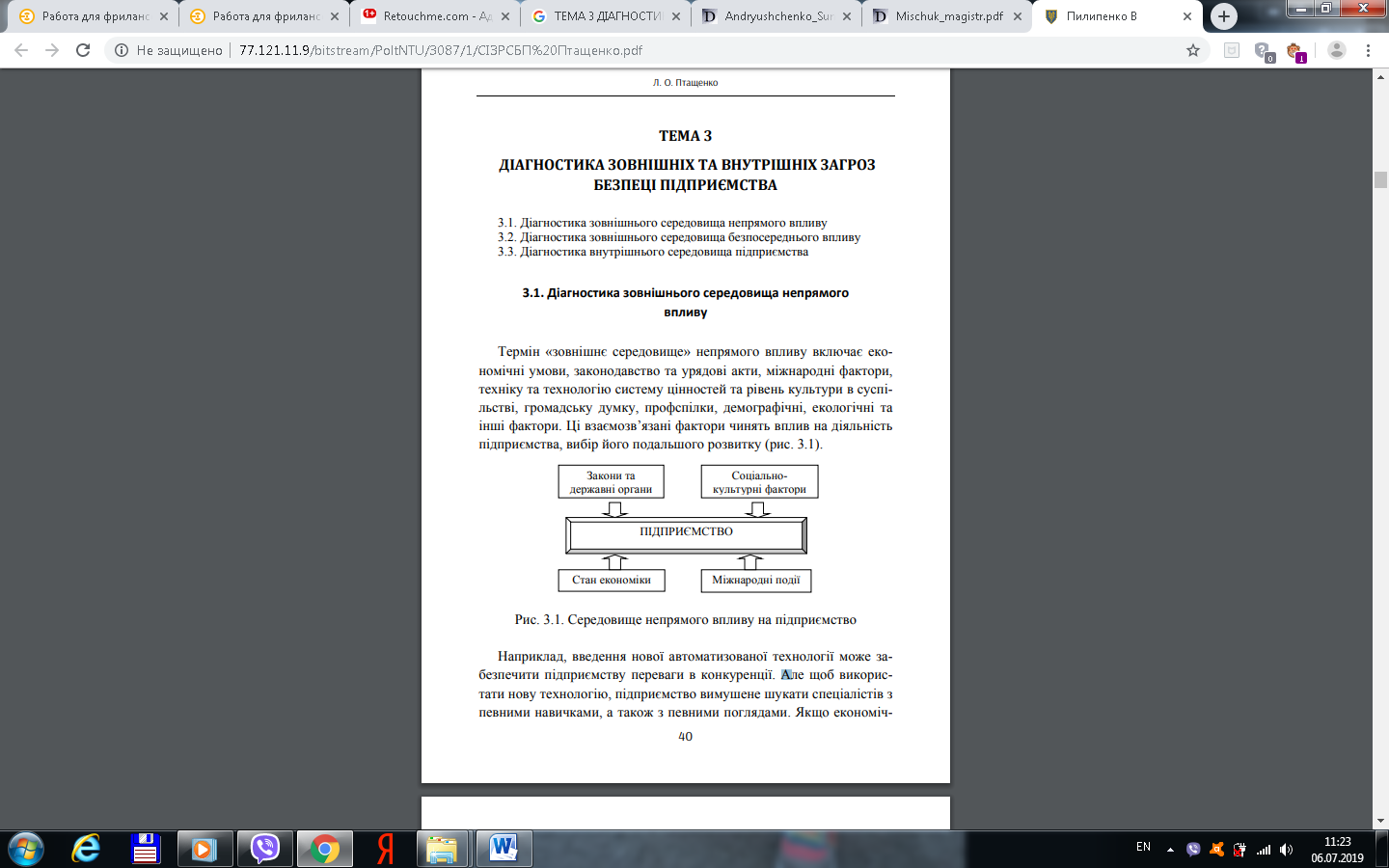
3. Діагностика внутрішнього середовища підприємства

**Вступ**

У сучасних умовах проблема економічної безпеки є актуальною, оскільки підприємства працюють в умовах різних зовнішніх і внутрішніх ризиків, а конкурентне економічне середовище приховує численні загрози. Ця обставина вимагає від суб'єктів управління підприємством побудови комплексної системи, спрямованої на підвищення рівня економічної безпеки. Проблема оцінки економічної безпеки держави, регіону, підприємства останнім часом набула особливої значущості. Однак, незважаючи на великий інтерес до неї вітчизняних та зарубіжних вчених і практиків, слід зазначити, що існуючі розробки в основному присвячені різним аспектам національної і регіональної безпеки, і в значно меншій мірі - питань економічної безпеки підприємств.

**1. Діагностика зовнішнього середовища непрямого впливу**

Термін «зовнішнє середовище» непрямого впливу включає економічні умови, законодавство та урядові акти, міжнародні фактори, техніку та технологію систему цінностей та рівень культури в суспільстві, громадську думку, профспілки, демографічні, екологічні та інші фактори. Ці взаємозв’язані фактори чинять вплив на діяльність підприємства, вибір його подальшого розвитку (рис. 1)

  
Рис. 1. Середовище непрямого впливу на підприємство

Наприклад, введення нової автоматизованої технології може забезпечити підприємству переваги в конкуренції. Але щоб використати нову технологію, підприємство вимушене шукати спеціалістів з певними навичками, а також з певними поглядами. Якщо економічна кон’юнктура підвищується та існує конкуренція на ринку таких спеціалістів, підприємство вимушене буде підняти заробітну плату, щоб залучити цих спеціалістів до роботи. Підприємство в процесі найму робітників має дотримуватися державного законодавства, яке забороняє дискримінацію за віком, статтю, расою. Усі ці фактори постійно змінюються.

З кожним роком керівництво вимушене враховувати все більшу кількість факторів зовнішнього середовища, які набувають глобального характеру. Всі підприємства залежать від зовнішнього середовища непрямої дії, яке, як правило, перебуває поза впливом менеджера (керівника). Але слід зазначити, що одні підприємства розвиваються та досягають успіху, а інші – банкрутують в одних і тих самих умовах. Діагностика середовища непрямого впливу на підприємство здійснюється шляхом оцінювання та аналізу економічних, технологічних, соціальних, політичних, ринкових, міжнародних факторів. У світовій економічній науці аналіз основних факторів зовнішнього середовища називається PEST-аналізом.

PEST – абревіатура назв різних середовищ:

P – political and legal environment (політико-правове середовище);

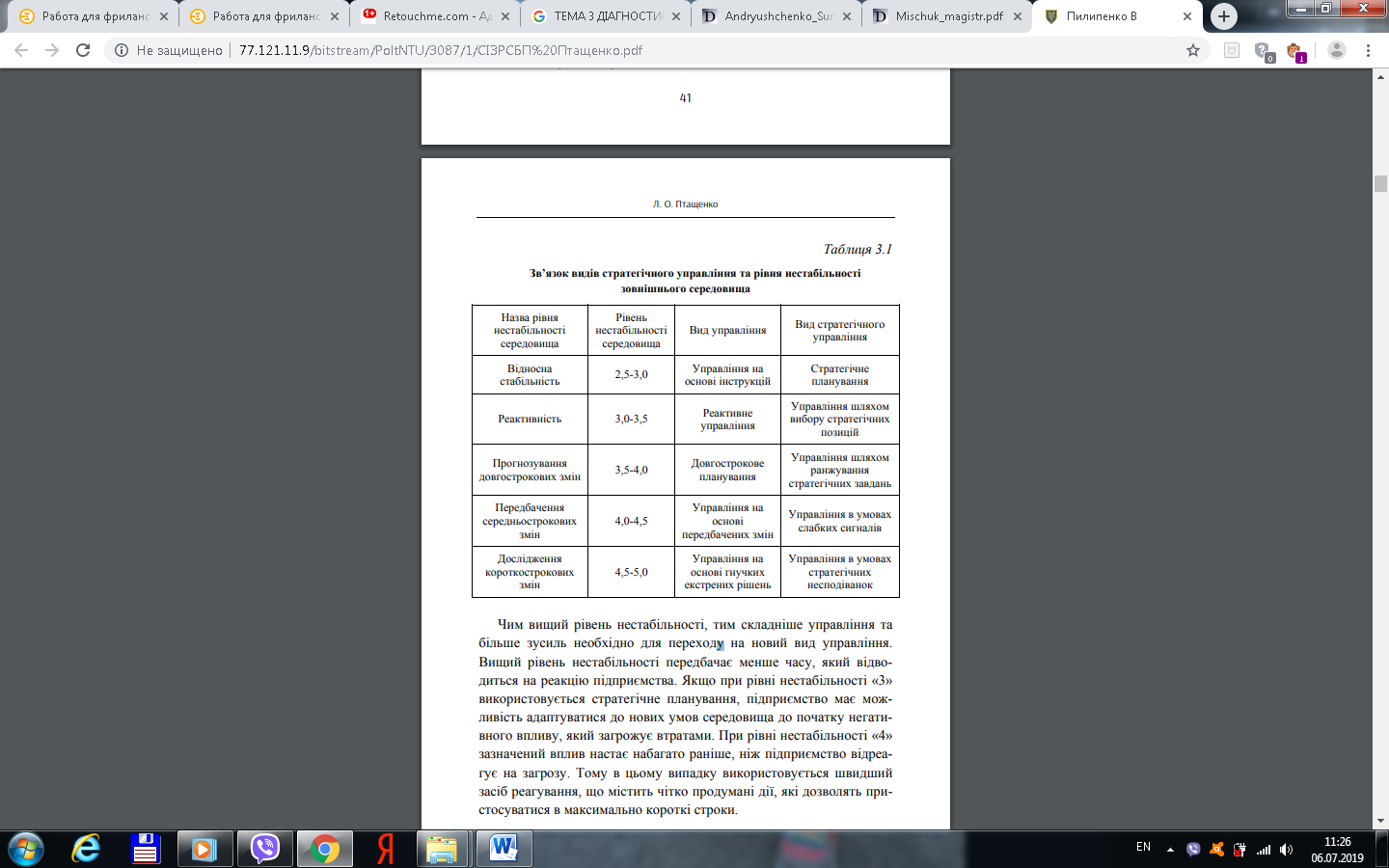
E – economic environment (економічне середовище);

S – sociocultural environment (соціокультурне середовище);

T – technological environment (технологічне середовище).

PEST-аналіз ставить за мету виявити ті фактори зовнішнього середовища, які найбільше впливають на підприємство, а також передбачити динаміку впливу цих факторів (сприятливу чи несприятливу). В процесі проведення діагностики зовнішнього середовища підприємства слід ураховувати рівень нестабільності. Рівень нестабільності залежить від галузі, в якій господарює підприємство, економічних і політичних факторів. Вибір виду стратегічного управління здійснюється відповідно до конкретного рівня нестабільності (табл.1).

Таблиця 1 Зв’язок видів стратегічного управління та рівня нестабільності зовнішнього середовища



Чим вищий рівень нестабільності, тим складніше управління та більше зусиль необхідно для переходу на новий вид управління. Вищий рівень нестабільності передбачає менше часу, який відводиться на реакцію підприємства. Якщо при рівні нестабільності «3» використовується стратегічне планування, підприємство має можливість адаптуватися до нових умов середовища до початку негативного впливу, який загрожує втратами. При рівні нестабільності «4» зазначений вплив настає набагато раніше, ніж підприємство відреагує на загрозу. Тому в цьому випадку використовується швидший засіб реагування, що містить чітко продумані дії, які дозволять пристосуватися в максимально короткі строки.

У випадку, коли рівень нестабільності дуже високий і наближається до «5», управління здійснюється на основі жорсткої координації дій і моментальної реакції на зміни. Такий вид управління називається стратегічним управлінням в умовах стратегічних несподіванок. У сучасних умовах рівень нестабільності дуже високий, тому використання стратегічного управління повинне враховувати зміни для забезпечення ефективного управління та розвитку підприємства. Розглянемо детальніше стратегічну оцінку зовнішнього середовища шляхом оцінювання названих факторів.

Політичні. Внутрішній ринок перебуває під впливом політичних подій та рішень. Відповідно до цього, політичні фактори відбиватимуться на операціях у галузі міжнародного бізнесу. Соціальне напруження може порушувати процес виробництва та обмежувати збут, якщо політичні рішення спрямовані проти якогось підприємства або продукту. Політичні дії проти уряду або раптова зміна режиму, як мінімум, збільшують невизначеність для експортера чи іноземного інвестора. Слід визнати, що такі події – винятки, а не правила. Майже в усіх країнах поточний політичний процес визначається певними змінами в державній політиці, а не переворотами. Проте навіть незначні зміни в політиці позначаються на бізнесі. Тому політичні фактори підприємство повинне враховувати до прийняття рішень щодо вкладання капіталів або прийняття на себе зобов’язань щодо збуту, тощо.

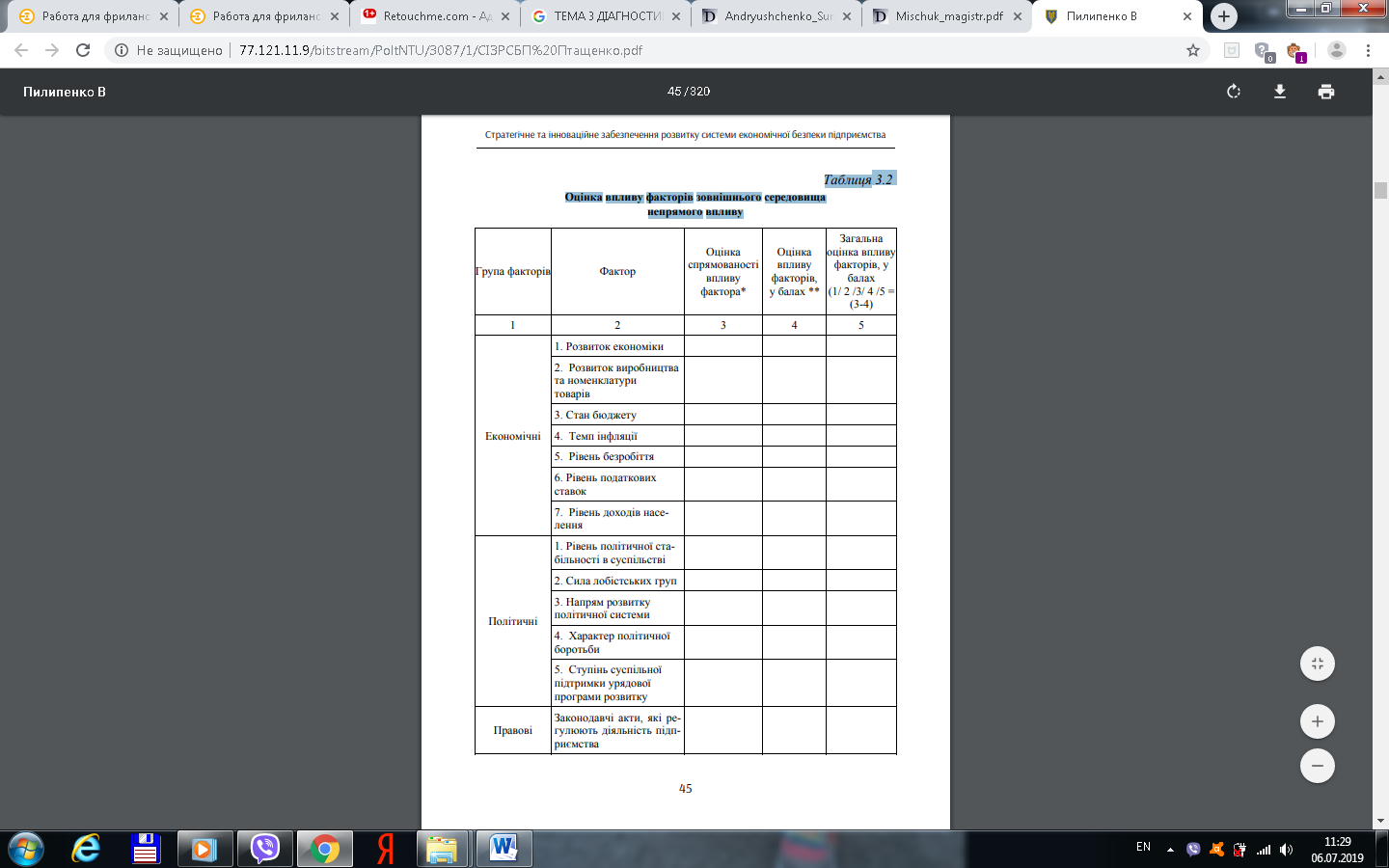
Правові. Займаючись господарською діяльністю, підприємство дотримується системи законодавчих актів. Кожне підприємство має відповідний правовий статус (приватне підприємство, акціонерне товариство, холдинг, корпорація, концерн, консорціум тощо). Саме цей факт визначає, як підприємство має вести справи, які податки сплачувати. Керівництво повинне дотримуватися законів чи нести відповідальність за їх недотримання, а в крайньому випадку навіть припиняти свою діяльність. Безумовно, розібратись у діючому законодавстві країни може лише кваліфікований юрист, до того ж українська законодавча база досить недосконала.

Економічні. Керівництво підприємства має враховувати тенденції змін в економіці при прийнятті рішень щодо перспектив діяльності. До економічних факторів, які можуть впливати на фінансово-господарську діяльність підприємства, можна віднести такі: рівень заробітної плати, транспортні тарифи, обмінний курс, рівень інфляції, ставки банківського відсотка, ВВП, податкова система, рівень економічного розвитку країни: чисельність населення, якість та кількість природних ресурсів, рівень розвитку технології тощо.

Соціокультурні. Виходячи з того, що підприємство здійснює свою діяльність у певному культурному середовищі, на неї впливає низка соціокультурних факторів: рівень освіти та професійної підготовки населення, життєві цінності, традиції. Від соціокультурних факторів залежать і способи ведення бізнесу деякими підприємствами. Від уявлень споживачів щодо якісного обслуговування залежить щоденна практика магазинів роздрібної торгівлі та ресторанів. Результатом соціокультурного впливу на організацію стала зростаюча увага до соціальної відповідальності. Керівництво має не тільки відстежувати соціальний вплив на підприємство, а й передбачати зміни в суспільстві та враховувати ці зміни більш ефективно, ніж конкуренти.

Технологічні. До технологічних факторів слід віднести державні та недержавні витрати на науку та техніку, патентно-ліцензійний захист технологій, нові тенденції в трансферті технологій, темпи розроблення нової продукції, інноваційні процеси. При діагностиці зовнішнього середовища важливо кількісно оцінити вплив кожного фактора за допомогою певної методики (табл. 2).

Таблиця 2 Оцінка впливу факторів зовнішнього середовища непрямого впливу



\* Оцінювання спрямованості впливу на підприємство здійснюється за такою оцінною шкалою:

+1 бал – позитивний вплив;

–1 бал – негативний вплив.

\*\* Оцінювання ступеня впливу фактора на підприємство здійснюється експертним шляхом за такою оцінною шкалою:

3 бали – сильний вплив;

2 бали – помірні впливи;

1 бал – слабкі впливи;

0 балів – відсутність впливу.

Для аналізу та діагностики впливу факторів зовнішнього середовища непрямого впливу визначається оцінка спрямованості впливу, оцінка ступеня впливу фактора та загальна оцінка впливу факторів на підприємство. За цією методикою можна виявити вплив кожного з факторів, порівняти вплив групи факторів, визначити загрози й можливості та оцінити в цілому ступінь впливу середовища на підприємство. Потрібно зазначити, що вплив факторів може оцінюватися як на рівні регіону, в якому здійснюється господарська діяльність підприємства, так і в Україні в цілому.

**2. Діагностика зовнішнього середовища безпосереднього впливу**

До факторів зовнішнього середовища підприємства безпосереднього впливу відносять фактори, які впливають на існування самого підприємства, на конкретні результати його діяльності (рис. 2).

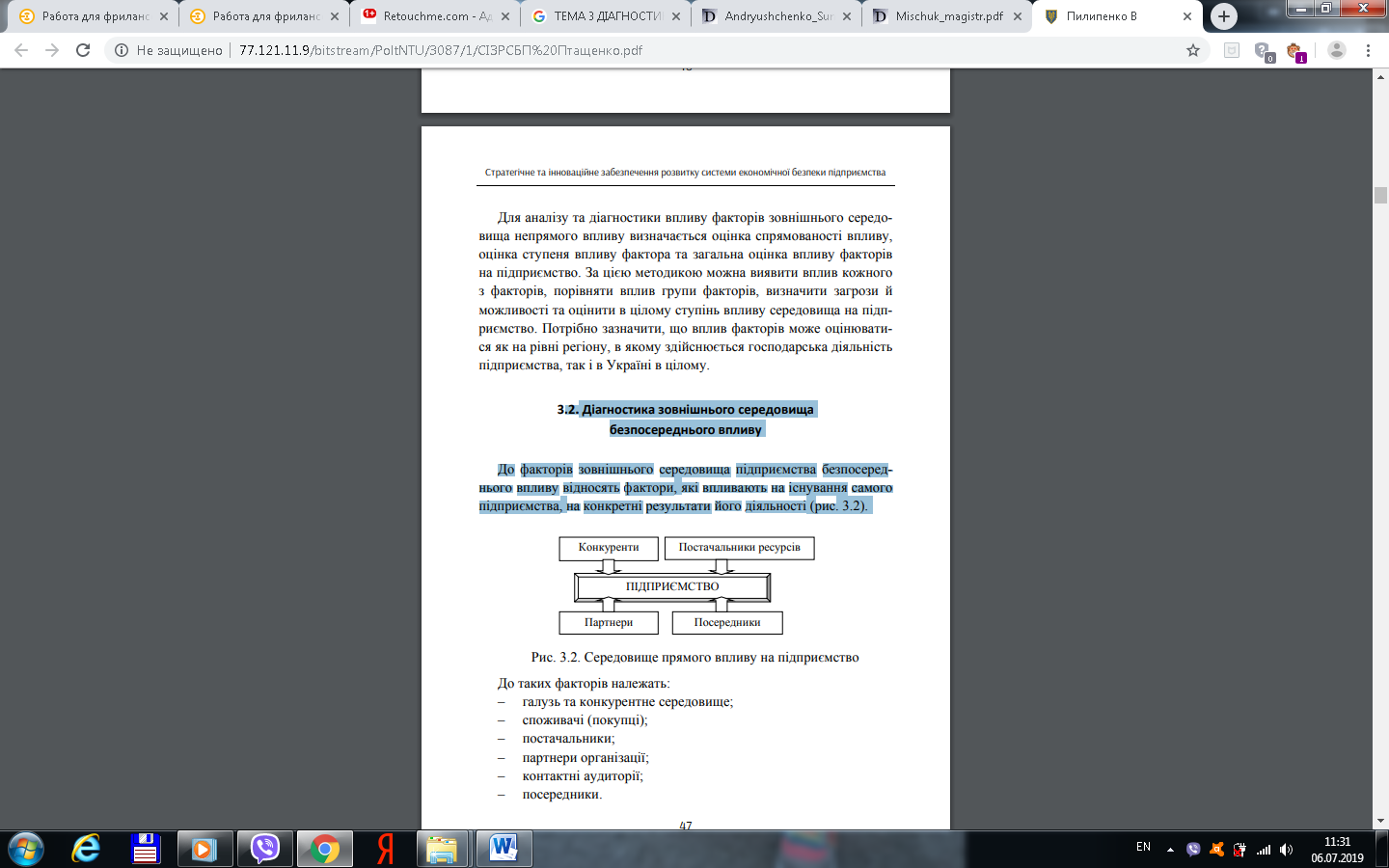


Рис. 2. Середовище прямого впливу на підприємство

До таких факторів належать:

– галузь та конкурентне середовище;

– споживачі (покупці);

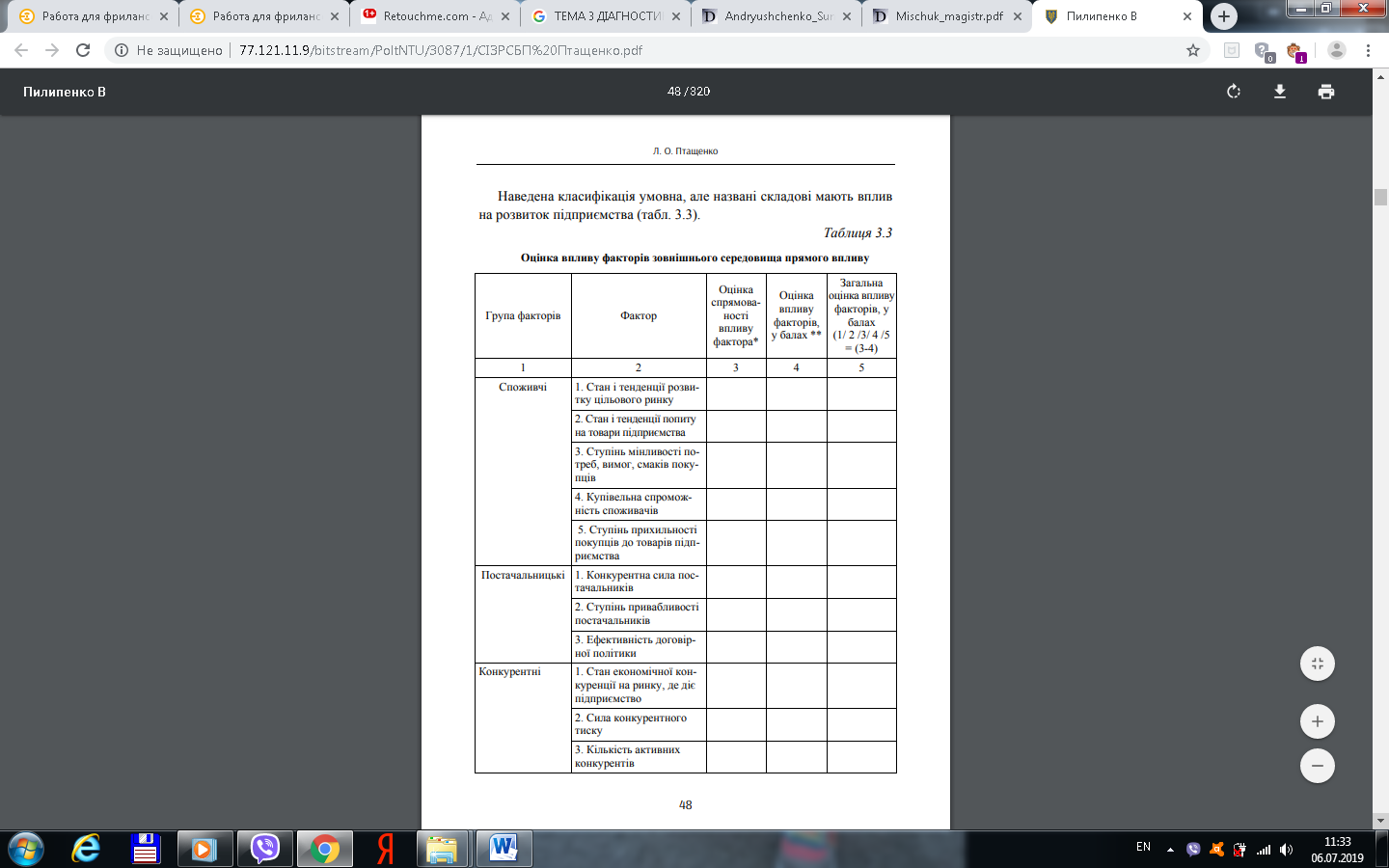
– постачальники; – партнери організації;

– контактні аудиторії;

– посередники.

Наведена класифікація умовна, але названі складові мають вплив на розвиток підприємства (табл. 3).

Таблиця 3 Оцінка впливу факторів зовнішнього середовища прямого впливу



\* Оцінювання спрямованості впливу на підприємство здійснюється за такою оцінною шкалою:

+1 бал – позитивний вплив;

–1 бал – негативний вплив.

\*\* Оцінювання ступеня впливу фактора на підприємство здійснюється експертним шляхом за такою оцінною шкалою:

3 бали – сильний вплив;

2 бали – помірні впливи;

1 бал – слабкі впливи;

0 балів – відсутність впливу.

Кожний з названих факторів середовища може призвести до банкрутства підприємства.

Наприклад, відсутність постачальника якогось конкретного матеріалу (обладнання) або несвоєчасність постачання можуть перешкодити випуску конкурентоспроможної продукції; сильні конкуренти можуть звести нанівець спроби фірми розширити сферу своєї діяльності тощо. Оцінювання впливу факторів зовнішнього середовища прямого впливу проводиться за аналогічною методикою (табл. 3).

Ця методика дозволяє виявити, порівняти вплив груп факторів, оцінити в цілому ступінь впливу, визначити загрози та можливості підприємства з найвпливовіших факторів даного середовища.

**3. Діагностика внутрішнього середовища підприємства**

Без діагностики внутрішнього середовища неможливо вибрати стратегію. Тільки докладний аналіз усіх аспектів діяльності підприємства дає змогу визначити сильні та слабкі його сторони, можливість реалізації обраного шляху розвитку.

Діагностика (від грец. diagnosis – розпізнавання) передбачає визначення суті та особливостей проблеми на основі всеохоплюючого аналізу, застосовуючи певний набір принципів та методів його проведення. Згідно з обраною методологією, діагностика потребує вибору, збирання та оброблення необхідної інформації з використанням методів аналізу та оцінювання, підготовки заходів для успішного розроблення стратегії. В процесі діагностики необхідно вивчити взаємозв’язки між загальними цілями підприємства, визначити та оцінити вплив складових середовища на результати його діяльності, а також визнати здатність підприємства здійснювати зміни.

Організація (підприємство, фірма) – це складна система, для діагностики якої використовується системний аналіз. Системний аналіз – це опис явища (ситуації) з певною метою з точки зору певної цілі (місії).

Система (грец. systema – буквально ціле зі складових частин) – сукупність, зумовлена правильним, закономірним розподілом частин у певному зв’язку. Наприклад, система управління підприємством може складатися з таких підсистем: – підсистема управління виробництвом; – підсистема управління маркетингом; – підсистема управління фінансами; – підсистема управління інноваційною діяльністю; – підсистема управління персоналом; – підсистема зовнішньоекономічної діяльності.

Отже, підсистема – це складова частина системи, яка має свої характерні, притаманні тільки їй, особливості. Вона взаємопов’язана з іншими підсистемами і її можна розглядати як самостійну систему (наприклад, маркетинг, фінанси, виробництво). Кожна підсистема складається з елементів.

Наприклад, підсистема управління виробництвом може складатися з таких елементів:

- управління основним виробництвом;

- управління допоміжним виробництвом;

- управління технологічною політикою підприємства;

- управління асортиментом продукції, яка виробляється;

- управління якістю продукції;

- управління плануванням випуску продукції;

- управління виробництвом нової продукції;

- управління ціноутворенням (тобто технічний ремонт, заміна матеріалів, технологічний прогноз і тощо);

- управління матеріалами, запасами тощо;

- управління цехами, відділами.

Існують різні методи виділення (декомпозиції) складу систем, які залежать від критерію декомпозиції.

Загальні критерії для декомпозиції підсистем:

– підсистеми можуть суттєво впливати на досягнення кінцевих результатів, цілей системи;

– підсистеми пов’язані із загальносистемною характеристикою, яка має необхідний та логічний зв’язок із досягненням цілей системи;

– підсистеми створюються за ознаками, які чітко проявляють необхідний функціональний зв’язок одних підсистем з іншими та системою в цілому;

– підсистеми пов’язані з поведінкою всіх елементів системи та відображають постійне функціонування взаємозв’язків елементів системи через її підсистеми з навколишнім середовищем. Декомпозиція підсистеми залежить від типу системи, мети діагностики та апарату аналізу.

Розглянемо характеристику елементів системи.

1. Елемент виступає структуротворчою частиною будь-якої системи (наприклад, підприємство є складовою галузі виробництва, з одного боку, та складається з цехів та служб – з іншого).

2. Елементу притаманні властивості, які будуть використовуватися системою або є потенційними для функціонального використання. Кожна властивість елемента може бути умовою для залучення його до системи.

3. Властивості елементів визначають їх місце у внутрішній організації системи. Елементи розвиваються в рамках системи та підкорюються умовам її функціонування, змінюючись у процесі розвитку системи або під тиском управлінського впливу.

4. Цілі системи визначають конкретну форму існування елементів як її (системи) частини. Тобто структурна автономність кожного елемента – одна з ознак елемента системи.

5. Елементи та підсистеми ніколи не діють самі по собі. Без взаємодії елементів не може до кінця реалізуватися функція кожного елемента (економісти, фінансисти, бухгалтери). Свою функцію й призначення елемент або підсистема може виконати тільки за умови, що буде взаємодіяти з елементами та підсистемами.

6. Взаємодія буде кращою, якщо будуть упорядковані взаємозв’язки елементів, підсистем.

Необхідно пам’ятати, що всі елементи, явища та процеси в системі взаємопов’язані й впливають одне на одного. Виділяючи будьяку підсистему, слід ураховувати вплив інших підсистем, зворотній вплив самої підсистеми на інші підсистеми. Тому вивчення та діагностика підсистеми повинні проводитись із урахуванням її зв’язків із зовнішнім середовищем. На базі взаємодії специфічних функцій кожної підсистеми вони об’єднуються в єдине ціле та утворюють систему.

Система – це не просто сума її елементів, а ціле, що має інші якості ніж складові елементи. Для того, щоб отримати правильний діагноз підприємства, потрібно провести дослідження підприємства системно, тобто необхідно проаналізувати комплекс взаємопов’язаних питань, що допоможе виявити об’єктивний стан системи управління та напрями її реорганізації. Глибокий і ретельний аналіз внутрішнього середовища є необхідною передумовою прийняття управлінських рішень.

Основним джерелом такого аналізу є економічна інформація – це конкретне відображення господарських процесів, що відбуваються всередині підприємства.

Без такої інформації та її аналізу неможливе ефективне функціонування й розвиток виробничо-збутової діяльності підприємства. Приймаючи стратегічні рішення, керівники підприємства повинні визначити: чи має підприємство внутрішні сили, щоб скористатися можливостями, і які внутрішні слабкості можуть ускладнити майбутні проблеми, пов’язані з зовнішніми небезпеками. Цим цілям слугує аналіз сильних і слабких сторін підприємства. Метод, що використовують для визначення внутрішніх проблем підприємства, називають управлінською діагностикою. Він заснований на комплексному дослідженні різних функціональних зон підприємства та в залежності від поставленого завдання, може методично бути простим чи складним.

Управлінський аналіз (діагностика) – це процес комплексного аналізу внутрішніх та зовнішніх ресурсів і можливостей підприємства, направлений замінити оцінку поточного стану бізнесу, його сильних і слабких сторін, виявлення стратегічних проблем.

Результати внутрішньої діагностики демонструють, наскільки ефективно проводиться управлінська діяльність сьогодні (які функції менеджменту чи маркетингу виконуються, хто їх виконує, наскільки ефективно вони виконуються – тобто чи є виправданими витрати часу та грошей на виконання).

Внутрішнє середовище (мікросередовище) можна досліджувати по ключових показниках (приміром, з допомогою портфельного аналізу оцінюється що випускає підприємство, асортимент товарів та послуг), або в розрізі функцій. Метод, що використовують для діагностики внутрішніх проблем, називають управлінським обстеженням.

Внутрішнє середовище має низку сегментів, кожен із яких містить набір ключових процесів і елементів підприємства, доходи, визначає той потенціал й ті можливості, якими володіє підприємство.

Кадровий сегмент внутрішнього середовища охоплює:

– взаємодію менеджерів та оптимізація працюючих;

– навчання й просування кадрів, бейнчмаркінг;

– оцінювання результатів праці та стимулювання;

– формування корпоративної культури й доброчесності у відносинах між працівниками тощо.

Організаційний сегмент включає:

– комунікаційні процеси та організаційні структури;

– норми, правила, процедури, ієрархію підпорядкування;

– розподіл правил і відповідальності.

У виробничий сегмент входять:

– виготовлення продукту, постачання і ведення складського господарства;

– обслуговування технологічного парку;

– здійснення досліджень і розробок.

Маркетинговий сегмент внутрішнього середовища підприємства охоплює всі ті процеси, котрі пов’язані з реалізацією продукції:

– стратегія продукту та стратегія ціноутворення;

– стратегія просування продукту на ринку;

– вибір ринків збуту та систем розподілу.

Фінансовий сегмент містить процеси, пов’язані із забезпеченням ефективного використання і рухом коштів підприємства, зокрема:

– підтримку ліквідності й забезпечення прибутковості;

– створення інвестиційних можливостей;

– формування ефективної політики управління активами й капіталом, тощо. Для цілей стратегічного планування під час обстеження фахівці рекомендують розглядати тільки п’ять функціональних зон – маркетинг, фінанси (управлінський і бухгалтерський облік), виробництво (операційний менеджмент), персонал, організаційну культуру й імідж підприємства тощо, проте стратегічні зміни можуть залежати від особливостей діяльності підприємства.

Внутрішня діагностика передбачає як аналіз поточної внутрішньої ситуації, так і розгляд її у стратегічному аспекті: наскільки параметри, що характеризують сильні й слабкі сторони підприємства, стабільні й стійкі в стратегічній перспективі, чи сильна стратегічна позиція є наслідком випадкового поєднання чинників, пов’язаних з ослаблення становища підприємства, з внутрішніми фундаментальними причинами, чи носить тимчасовість.

З іншого боку, внутрішня діагностика проводиться з метою оцінювання наслідків здійснюваних стратегічних змін. Виявивши сильні й слабкі сторони, і зваживши чинники за рівнем значимості, керівництво може впливати на ті функціональні зони, які вимагають негайного втручання чи можуть почекати, або на ті, куди можна використати розробки стратегії підприємства.

Діагностика за слабкими сигналами. Сутність цього методу діагностики полягає в тому, щоб вчасно визначити слабкі сигнали – ранні й неточні ознаки настання кризових ситуацій – і вчасно відреагувати на них. Необхідність діагностики по слабких сигналах виникає в ситуації, коли рівень нестабільності середовища підприємства надзвичайно високий. Шкала, що дозволяє оцінити рівень нестабільності в балах, представлена на рис. 3. Високому рівню нестабільності відповідають 4–5 балів.

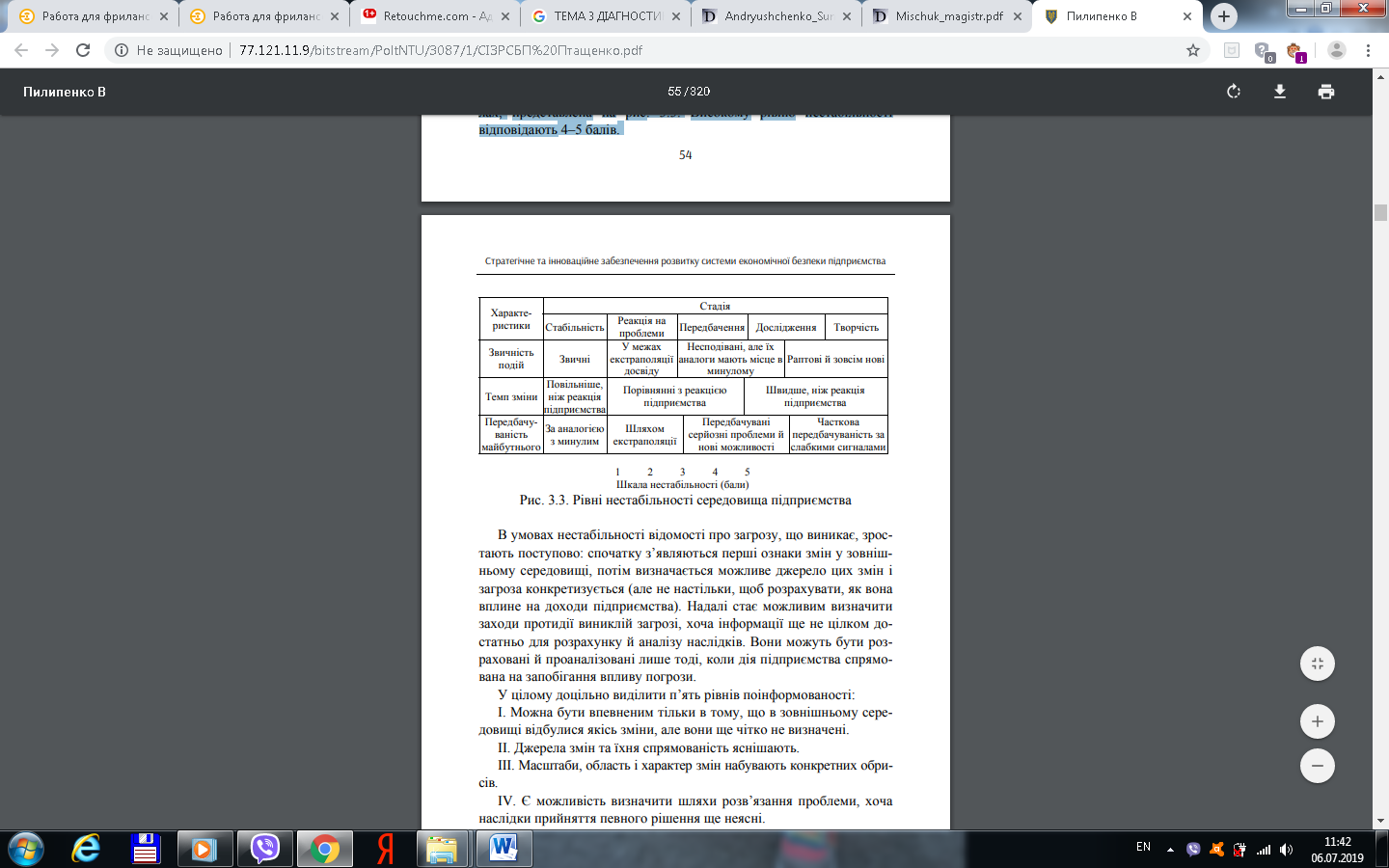


Рис. 3. Рівні нестабільності середовища підприємства

В умовах нестабільності відомості про загрозу, що виникає, зростають поступово: спочатку з’являються перші ознаки змін у зовнішньому середовищі, потім визначається можливе джерело цих змін і загроза конкретизується (але не настільки, щоб розрахувати, як вона вплине на доходи підприємства). Надалі стає можливим визначити заходи протидії виниклій загрозі, хоча інформації ще не цілком достатньо для розрахунку й аналізу наслідків. Вони можуть бути розраховані й проаналізовані лише тоді, коли дія підприємства спрямована на запобігання впливу погрози.

У цілому доцільно виділити п’ять рівнів поінформованості:

1. Можна бути впевненим тільки в тому, що в зовнішньому середовищі відбулися якісь зміни, але вони ще чітко не визначені.

2. Джерела змін та їхня спрямованість яснішають.

3. Масштаби, область і характер змін набувають конкретних обрисів.

4. Є можливість визначити шляхи розв’язання проблеми, хоча наслідки прийняття певного рішення ще неясні.

5. Результати прийнятих рішень по усуненню небезпеки можна передбачати, і вони стають певними. Таким чином, для того щоб вчасно реагувати на сигнали, які надходять як ззовні, так і з внутрішнього середовища, в рамках системи контролінгу повинно бути організоване спостереження за більшою кількістю параметрів, що характеризують умови життєдіяльності підприємства.

Це складно, але складність проблеми не може бути виправданням для відмови від її розв’язання. Найбільш доцільним напрямом для організації контролю за параметрами зовнішнього й внутрішнього середовищ є проведення моніторингу – безперервного систематичного спостереження за параметрами зовнішнього й внутрішнього середовищ підприємства, збору й аналізу зібраної інформації.

Моніторинг повинен складатися з таких елементів:

– перелік спостережуваних цільових критеріїв оцінки діяльності підприємства;

– принципи кількісної та якісної оцінок зовнішніх сигналів;

– принципи кількісної та якісної оцінок внутрішніх сигналів;

– періодичність спостереження встановлених критеріїв;

– методи аналізу можливих наслідків, виявлених у процесі спостереження вихідних економічних явищ і породжуваних ними ланцюжків економічних явищ;

– методи визначення «контрольних точок» у ланцюжках економічних явищ і порядок спостереження за цими точками;

– методи економічного аналізу всередині підприємства, узагальнення результатів спостереження динаміки значення критеріїв;

– принципи вироблення антикризових управлінських рішень на підставі результатів спостережень та економічного аналізу;

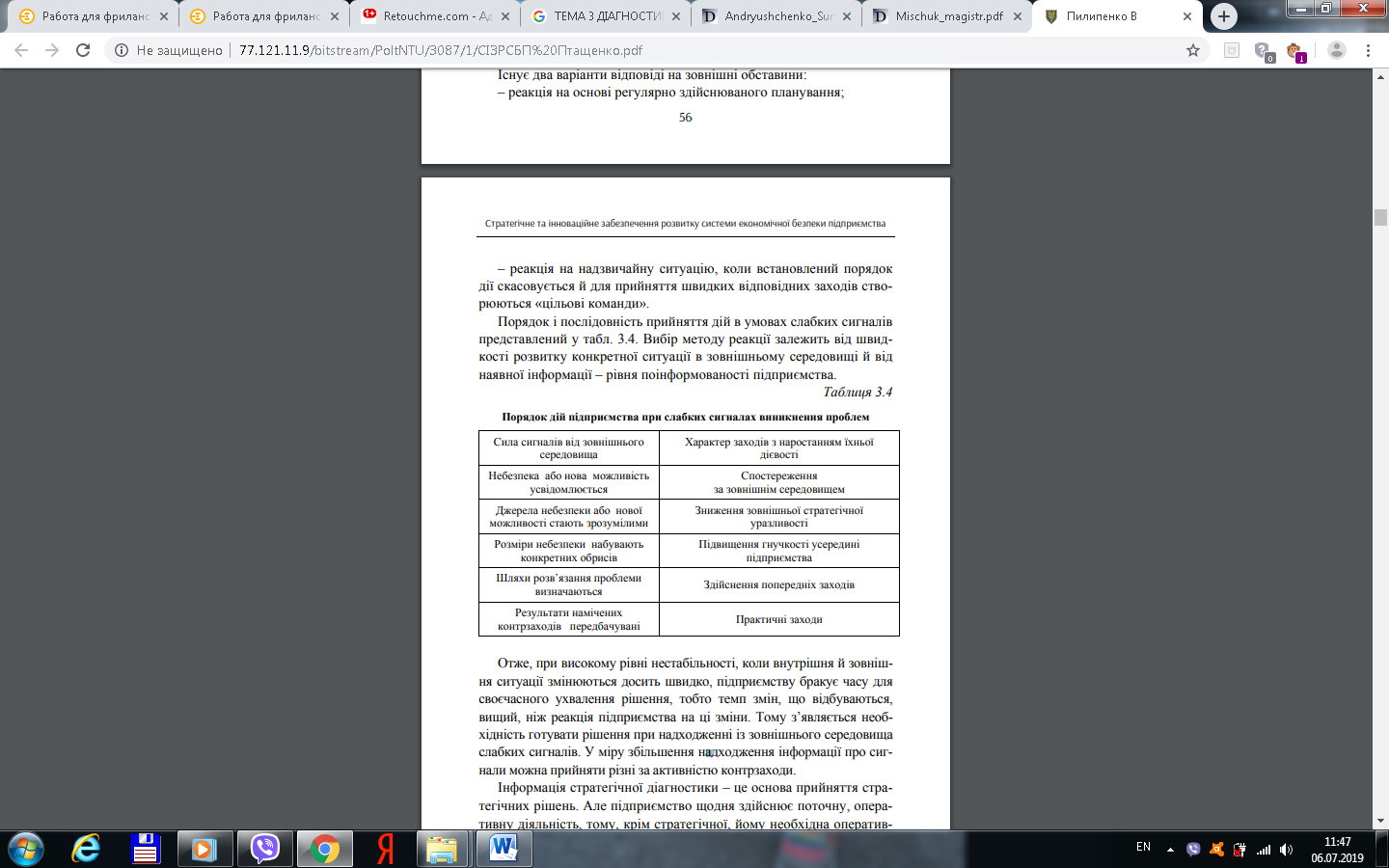
– порядок проходження перелічених розділів відображає порядок проведення комплексу дослідження зовнішнього й внутрішнього середовищ підприємства й вироблення на цій основі управлінських рішень.

Моніторинг «вилучає» сильні й слабкі сигнали, які надходять не із внутрішнього, а із зовнішнього середовища. Відразу після одержання сигналу відповідна служба розробляє пропозиції про можливу реакцію на нього. Існує два варіанти відповіді на зовнішні обставини:

– реакція на основі регулярно здійснюваного планування;

– реакція на надзвичайну ситуацію, коли встановлений порядок дії скасовується й для прийняття швидких відповідних заходів створюються «цільові команди». Порядок і послідовність прийняття дій в умовах слабких сигналів представлений у табл.4. Вибір методу реакції залежить від швидкості розвитку конкретної ситуації в зовнішньому середовищі й від наявної інформації – рівня поінформованості підприємства.

Таблиця 4 Порядок дій підприємства при слабких сигналах виникнення проблем



Отже, при високому рівні нестабільності, коли внутрішня й зовнішня ситуації змінюються досить швидко, підприємству бракує часу для своєчасного ухвалення рішення, тобто темп змін, що відбуваються, вищий, ніж реакція підприємства на ці зміни. Тому з’являється необхідність готувати рішення при надходженні із зовнішнього середовища слабких сигналів. У міру збільшення надходження інформації про сигнали можна прийняти різні за активністю контрзаходи.

Інформація стратегічної діагностики – це основа прийняття стратегічних рішень. Але підприємство щодня здійснює поточну, оперативну діяльність, тому, крім стратегічної, йому необхідна оперативна діагностика фінансово-господарського стану.

**Висновок.**

Термін «зовнішнє середовище» непрямого впливу включає економічні умови, законодавство та урядові акти, міжнародні фактори, техніку та технологію, систему цінностей та рівень культури в суспільстві, громадську думку, профспілки, демографічні, екологічні та інші фактори. До факторів зовнішнього середовища підприємства безпосереднього впливу відносять фактори, які впливають на існування самого підприємства, на конкретні результати його діяльності. Внутрішня діагностика передбачає як аналіз поточної внутрішньої ситуації, так і розгляд її у стратегічному аспекті: наскільки параметри, що характеризують сильні й слабкі сторони підприємства, стабільні й стійкі в стратегічній перспективі, чи сильна стратегічна позиція є наслідком випадкового поєднання чинників, пов’язаних з ослаблення становища підприємства, з внутрішніми фундаментальними причинами, чи носить тимчасовість.

**Завдання для самостійної роботи**

1. Особливості формування служби економічної безпеки підприємства на вітчизняних підприємствах.

2. Як повинні забезпечувати належний рівень економічної безпеки підприємства основні його підрозділи?

3. Як захиститись від неправомірних дій контрагентів підприємства?

4. Як сформувати систему показників для проведення оцінки та аналізу економічної безпеки підприємства?

5. Проаналізувати взаємозв’язок та взаємообумовленість складових інформаційно-аналітичного забезпечення економічної безпеки підприємства.

**Питання для самоконтролю**

1. Визначте сутність PEST-аналізу.

2. Оцінювання яких факторів формує стратегічну оцінку зовнішнього середовища підприємства?

3. Визначте сутність системи та її складових в управлінні економічною безпекою підприємства.

4. У чому виявляється проведення діагностики за слабкими сигналами?

5. Який елемент діагностики доцільно застосовувати для організації контролю за параметрами зовнішнього й внутрішнього середовищ підприємства та в чому він полягає?

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Птащенко Л. О. Фінансовий контролінг [текст] навч. посіб. / Л. О.Птащенко, В. В.Сержанов. – К.: «Центр учбової літератури», 2016. – 344с. Ptashchenko L., Serzhanov V. Financial Controlling: [Tutorial] / L. Ptashchenko, V. Serzhanov – K.: Center of educational literature, 2016. – 344 years

2. Мехеда Н. Г., Савченко А. П. Вплив зовнішнього середовища на діяльність підприємства [Електронний ресурс]. Режим доступу: <http://www.rusnauka.com/15_NNM_2014/Economics/10_170149.doc.htm>

3. Яковлєв Ю. П. Контролінг на базі інформаційних технологій К.: Центр навчальної літератури, 2006. – 318 с.

**Лекція №8**

**Тема. Моделі побудови системи корпоративної безпеки**

**Мета:** визначення алгоритму моделі забезпечення безпеки, теоретичних основ моделювання діяльності по реалізації державної. економічної політики в сфері інновацій та інвестицій.

**План**

1. Алгоритм моделі забезпечення безпеки.

2. Механізми забезпечення безпеки соціальної системи - організації, сутність і завдання.

3. Теоретичні основи моделювання діяльності по реалізації державної. економічної політики у сфері інновацій та інвестицій.

**1. Алгоритм моделі забезпечення безпеки.**

Моделювання в широкому сенсі є методом наукового пізнання. На практиці моделювання використовується при організації, плануванні, вдосконаленні конкретних видів діяльності. Моделювання передбачає побудову певного способу досліджуваного об 'єкта (предмета, процесу або явища), що представляє собою систему елементів, що відтворюють його основні характеристики (сторони, зв'язку, функції і т. п.). Аналогія між досліджуваним об 'єктом і моделлю дозволяє переходити від моделі до самого об' єкту і переносити на нього результати, отримані при дослідженні моделі. В даному випадку об 'єктом дослідження є діяльність органів державної влади та суб'єктів господарювання щодо забезпечення економічної безпеки, модель якої необхідно побудувати.

У відповідності з системним підходом, модель діяльності щодо забезпечення економічної безпеки в якості своїх елементів має, на наш погляд, включати:

- цілі та завдання діяльності;

- суб'єкт діяльності;

- об'єкт діяльності та його основні особливості;

- загрози об'єкту захисту та механізми їх реалізації.

- умови, в яких ця діяльність здійснюється (або особливості середовища);

– форми, методи та засоби, що використовуються суб'єктами діяльності для досягнення своїх цілей і вирішення конкретних задач;

- тактика використання сил і засобів для захисту інтересів;

- результат діяльності як прогнозована форма досягнення мети.

Вихідним моментом моделювання є визначення цілі такої діяльності. На нашу думку, вона формулюється у визначенні економічної безпеки. На відміну від існуючих підходів визначення економічної безпеки, робить акцент на тому, що - це стан системи економічних відносин між суб 'єктами господарювання, індивідами, урядовими інституціями як в рамках Національної економіки, так і в інших сферах економічної діяльності, що забезпечує можливість повної реалізації і захищеність життєво важливих економічних інтересів від зовнішніх і внутрішніх загроз через усунення передумов і подолання існуючих протиріч, досягнення збалансованості інтересів кожного з учасників економічних відносин. Тобто, має бути побудована модель діяльності, яка буде забезпечувати такий стан системи економічних відносин.

Забезпечення економічної безпеки - це діяльність по створенню умов для стабільного безкризового розвитку економічної системи, виявлення, попередження і припинення загроз, усунення протиріч між інтересами різних держав, соціальних груп, суспільства та індивіда.

Головною метою забезпечення Національної економічної безпеки є дозвіл протиріч між економічними інтересами суб 'єктів господарювання, держави, особистості і суспільства, між інтересами різних держав у сфері міжнародних економічних відносин, створення сприятливих умов для еквівалентної, рівноправній реалізації життєво важливих економічних інтересів всіх суб' єктів економічних відносин.

Забезпечення економічної безпеки являє собою цілеспрямовану, постійно яка здійснюванюється діяльність (господарську, нормотворчу, аналітичну, організаційну, оперативно-розшукову та іншу) всіх суб’єктів економічної безпеки щодо захисту життєво важливих економічних інтересів. Основними етапами якої є: вичленення життєво важливих економічних інтересів в кожній сфері господарської діяльності; створення механізмів прогнозування і виявлення загроз; формування системи протидії чинним та із виниклих загроз; розробка механізмів взаємодії всіх суб 'єктів системи безпеки.

Система забезпечення економічної безпеки включає в себе сукупність суб'єктів економічної безпеки, систему заходів і діяльність щодо їх реалізації в цілях захисту життєво важливих економічних інтересів особистості, суспільства і держави від зовнішніх і внутрішніх загроз.

Суб'єктами забезпечення економічної безпеки є держава і його структури, юридичні та фізичні особи, інші суб' єкти господарювання.

Основним суб'єктом економічної безпеки, що забезпечує її реалізацію на національному, громадському, державному рівні, а так само, що справляє істотний вплив на реалізацію економічної безпеки особистості (громадян) є держава, яка здійснює функції в даній області через органи законодавчої, виконавчої та судової влади.

Юридичні та фізичні особи (громадяни) забезпечують своєю діяльністю, власну економічну безпеку, захищаючи і реалізовуючи життєво важливі економічні інтереси, але також зобов'язані відповідно до цього Закону, законами та іншими нормативними актами України, що регулюють відносини у сфері економічної діяльності, не допускати ущемлення національних і державних інтересів, забезпечувати умови для їх пріоритетною реалізації.

В систему органів, що забезпечують національну економічну безпеку (або іншими словами - суб 'єктами системи забезпечення економічної безпеки є: Президент, Кабінет Міністрів, органи законодавчої і виконавчої влади всіх рівнів, Міністерства і відомства, підприємства та установи різних форм власності, юридичні та фізичні особи.

Система забезпечення Національної економічної безпеки об'єднує цілеспрямовану діяльність державних органів, посадових осіб та громадян України щодо захисту життєво важливих економічних інтересів особистості, суспільства і держави від усіх видів загроз зовнішнього і внутрішнього характеру.

Для забезпечення Національної економічної безпеки даними суб'єктами здійснюється система заходів (правового, економічного, організаційного, аналітичного, оперативно-розшукового та іншого необхідного для захисту економічних інтересів характеру), що включає в себе: розробку економічних механізмів регулювання системи економічних відносин у суспільстві; прийняття правових, нормативних актів, що закріплюють сформовану систему економічних відносин і регулюючих практику господарської діяльності; здійснення організаційних та управлінських дій, що забезпечують функціонування всіх суб'єктів господарювання і ефективну, еквівалентну реалізацію їх інтересів.

Предметом державної діяльності в галузі забезпечення Національної економічної безпеки є:

- визначення і моніторинг факторів, що підривають стійкість соціально-економічної системи і держави в короткостроковій та довгостроковій перспективі;

- формування та проведення економічної політики (визначення цілей, пріоритетів, завдань і напрямів забезпечення економічної безпеки).

Пріоритетні напрями забезпечення Національної економічної безпеки повинні формулюватися в програми (стратегії) забезпечення економічної безпеки України.

Програма (стратегія) забезпечення економічної безпеки України - це система політичних, економічних, організаційних, правових заходів, що забезпечують включення національних життєво важливих економічних інтересів суспільства і всіх громадян, підприємств, міністерств і відомств, суб'єктів господарювання та загроз їм на даному історичному відрізку часу в умовах нинішній зовнішньополітичній, соціально-економічної обстановці. Програма (стратегія) може включати характеристику умов, факторів і найважливіших параметрів та порогових показників, досягнення яких забезпечить умови для реалізації всієї системи національних життєво важливих економічних інтересів.

На основі програми (стратегії) Міністерства і відомства повинні готувати плани заходів щодо забезпечення економічної безпеки у відповідній сфері економічної діяльності.

Кожен з суб’єктів забезпечення економічної безпеки виконує свої функції у певній сфері господарської, управлінської або організаційної діяльності, реалізує діяльність щодо забезпечення економічної безпеки за рахунок розробки заходів економічного, правового, аналітичного, оперативно-розшукового та іншого характеру відповідно з компетенцією покладеного на нього законодавством України.

Програма (стратегія) забезпечення економічної безпеки становить основу планування діяльності кожного суб'єкта. Зміст цієї діяльності визначається моделлю, що розробляється кожним із суб'єктів:

- умов тій сфері господарського життя, в якій цей суб'єкт здійснює свою діяльність;

- наявних у розпорядженні суб'єкта механізмів, засобів і заходів протидії загрозам, можливостей їх запобігання;

- функцій, які те чи інший структурний підрозділ виконує в межах господарської діяльності.

Побудова системи забезпечення економічної безпеки, так само як і Національної безпеки, в усіх її складових, повинно базуватися, на наш погляд, на методологічному підході, що включає в якості елементів системи забезпечення безпеки:

- виявлення загроз та суб 'єктів загроз економічній безпеки у сучасних умовах;

- визначення об'єктів захисту;

- механізм виявлення життєво важливих економічних інтересів країни або суб'єкта господарювання, сфер і особливостей їхньої реалізації;

- виявлення суб'єктів, чия діяльність завдає шкоди життєво важливим економічним інтересам особистості, підприємства, суспільства і держави;

- визначення ознак, що свідчать про вчинення дій, що завдають шкоди життєво важливим економічним інтересам країни або суб'єкта господарювання;

- визначення основних факторів і умов, які виникають у сфері забезпечення економічної безпеки держави або підприємства;

- аналіз особливостей і механізмів нанесення шкоди життєво важливим економічним інтересам країни або господарюючим суб 'єктам;

- визначення компетенції та взаємовідносин органів, які провадять діяльність із забезпечення економічної безпеки;

- формування системи заходів щодо реалізації життєво важливих економічних інтересів;

- діяльність з протидії загрозам і локалізації їх наслідків.

Слід підкреслити, що ефективність діяльності щодо забезпечення економічної безпеки буде тим вище, чим більш чітко будуть визначені об'єкт захисту і погрози. Саме від визначення того, що необхідно захищати і від чого залежить зміст програми (стратегії) діяльності кожного суб'єкта системи забезпечення економічної безпеки.

Відповідно досягнення економічної безпеки пов'язувалося з таким станом економіки, коли негативний вплив ззовні нейтралізувати компенсуючими резервами господарства країни, і зберігалася економічна, соціальна і політична стабільність. З такого формулювання витікало, що забезпечення економічної безпеки реалізується як процес розробки системи заходів щодо стабілізації економічного становища, але не передбачалася діяльність із запобігання загроз.

На наш погляд, слід звернути увагу на те, що на всіх рівнях або держави, або підприємства, підходи до забезпечення економічної безпеки практично базуються на виокремлення в якості об'єкта економічної безпеки тих чи інших проблем, вирішення яких є життєво важливим економічним інтересом. Іншими словами, фактично реалізується загальний методологічний підхід до побудови концепції економічної безпеки на основі аналізу реально існуючих життєво важливих економічних інтересів і відносин як об'єкта економічної безпеки.

В загальному плані економічні інтереси визначаються як сукупність потреб, що формуються у індивідів, соціальних спільностей та інших суб'єктів господарювання під впливом системи економічних відносин і що спонукають їх до активної господарської діяльності. Задоволення важливих, значущих потреб обумовлює процес функціонування й розвитку, як світової економіки, економік окремих країн, так і життєдіяльності окремого індивіда виробника. Тому життєво важливі національні економічні інтереси можуть бути визначені як сукупність потреб, задоволення яких забезпечує життєдіяльність особистості, підприємства, товариства і держави в даний проміжок часу.

В системі економічних інтересів:

- необхідно створити ієрархію інтересів - виокремлювати довгострокові, перспективні і короткострокові, але не менш життєво важливі інтереси.

Не менш важливе методологічне значення для побудови системи забезпечення економічної безпеки поряд з її об'єктом набуває питання про реальні та потенційні загрози життєво важливим економічним інтересам, умовам і можливостям їх реалізації. Розробка концепції повинна ґрунтуватися на обліку всього комплексу загроз економічній безпеки. Інакше система забезпечення економічної безпеки буде запізнюватися із заходами захисту або приймати неадекватні загрозам дії.

Концепція ООН, наприклад, в якості загроз економічній безпеки держав розглядає такі фактори як:

• незабезпеченість економіки сировиною і енергоресурсами;

• незабезпеченість продуктами харчування;

• нераціональна експлуатація природних ресурсів;

• незабезпеченість виробничо-технічних та науковим потенціалом;

• стихійні лиха (неврожаї, землетруси, повені, посухи та інші фактори природного характеру);

• деградація навколишнього середовища;

• механізм функціонування системи міжнародної торгівлі, заснований на neekvivalentnom обміні;

• протекціоністські заходи, блокади і ембарго, використовувані в політичних цілях;

• нестабільність цін на сировину;

• недоліки системи приватного фінансування, що призводять до кризи заборгованості;

• часті коливання процентних ставок;

• обмеження з політичних причин доступу на ринки кредитів;

• обмеження обсягу допомоги;

• недосконалість механізму прийняття рішень, що регулює функціонування валютної системи та ін.

Немає необхідності заперечувати проти виокремлення цих загроз економічної безпеки. Але слід враховувати, що вони сформульовані, виходячи з потреб країн, що розвиваються, і зачіпають, перш за все, систему міжнародних економічних відносин. Стосовно до нинішньої ситуації в Україні мову слід вести про те, що поряд із зовнішніми загрозами на економічну безпеку більшою мірою роблять вплив внутрішні загрози, зумовлені наявністю і загостренням протиріч всередині держави.

В якості деяких таких процесів і факторів, що негативно впливають на економічну безпеку України та виробників в сучасних умовах повинні розглядатися:

• розрив господарських зв'язків у виробничій сфері і бурхливий розвиток зв'язків у сфері перекуповування і перепродажу;

• значне зростання тіньової економіки, криміналізація економіки, зростання економічної злочинності.

• інфляція;

• "Чорнобильський" фактор та інші.

У цьому зв 'язку, мабуть, доцільно проводити більш детальну класифікацію факторів економічної безпеки, що дозволить підійти до проблеми її забезпечення з урахуванням ситуації в країні.

Однією з підстав такої класифікації може стати вичленення факторів, що впливають на реалізацію економічних інтересів. До другої групи факторів, на наш погляд, відносяться фактори, що забезпечують стійкість економічного розвитку. Третя група, - фактори, що створюють умови для виникнення сфер більш імовірнісного завдання економічної збитку. Мабуть, доцільно проводити класифікацію і за такою підставою як ставлення до компетенції тих чи інших елементів державного апарату щодо забезпечення економічної безпеки. Така класифікація, на нашу думку, дозволить більш детально врахувати всі фактори при організації системи забезпечення економічної безпеки країни, розмежувати компетенцію державних органів і сформулювати завдання щодо забезпечення економічної безпеки на найближчу і віддалену перспективу.

В якості суб'єктів загроз економічній безпеки, чиї конкретні дії завдають шкоди життєво-важливим економічним інтересам stragny, слід, на наш погляд, розглядати:

- юридичних осіб (підприємці, фірми, фонди та благодійні організації; державні підприємства та інші суб’єкти господарювання);

- фізичних осіб, професійно які виконують роботу економічного характеру (приватні виробники і підприємці, що не мають статусу юридичної особи; керівники, які здійснюють від імені підприємств господарські операції; співробітники державних організацій та установ тощо);

- іноземних юридичних осіб, організації, фірми, спецслужби і т. д.;

- організовану злочинність, діючу як всередині країни, так і за кордоном.

Слід враховувати, що всі суб'єкти господарювання можуть мати що суперечать загальнонародним і державним особисті, корисливі економічні інтереси і використовувати форми, методи діяльності, які їм дозволяють досягти потрібного результату. І в цьому відношенні вони функціонують у рамках прав, наданих їм Конституцією. Однак з іншого боку, їхні дії можуть ущемляти життєво важливі економічні інтереси суспільства, держави або інших суб 'єктів господарювання, тобто бути загрозою економічної безпеки Республіки або окремого виробника. Іншими словами, вони реально виступають суб 'єктами загроз економічної безпеки. Тому при оцінці даних суб 'єктів як носіїв загроз в сучасних умовах слід виходити з критерію відповідності їх діяльності встановленим правовим, господарським нормам і правилам.

Відповідно, у вузькому розумінні, як економічна безпека підприємства, галузі, регіону або суб'єктів господарювання - це захищеність виробничих, фінансових, юридичних та інших відносин і організаційних зв'язків, матеріальних, фінансових та інтелектуальних ресурсів, при якому реалізовуються їхні економічні інтереси.

Структурний аспект проблеми передбачає виділення основних факторів, що впливають на економічну безпеку держави та суб'єктів господарювання. Ці фактори можна розділити на групи, що характеризують: матеріальне забезпечення виробництва; стан робочої сили, розміри і прогресивність основного виробничого капіталу (фондів); розвиток сфери досліджень, розробка технологічних нововведень, можливість збуту продукції на зовнішньому і внутрішньому ринках і ряд інших.

На рівні суб'єктів господарювання економічна безпека як стан - це наявність таких економічних, виробничих і технологічних умов, які дозволяють забезпечувати законну реалізацію економічних інтересів без виникнення суперечностей з інтересами інших суб'єктів і стійко функціонувати в даний момент.

У функціональному плані економічна безпека тотожна поняттю "забезпечення економічної безпеки" і повинна розглядатися як процес забезпечення, досягнення єдності життєво важливих інтересів; виявлення і попередження загроз їм; протидії суб'єктам загроз, що фактично буде забезпечувати створення і зміцнення умов надійного функціонування Національної економіки в ході її розвитку.

Варто окремо зупинитися на такому етапі діяльності як формування і здійснення системи заходів щодо реалізації життєво важливих економічних інтересів. Для кожної держави ця система заходів повинна передбачати заходи щодо забезпечення стабільного функціонування економіки і забезпеченню її необхідного розвитку. Проблема в даному випадку полягає в тому, що найчастіше підтримка стабільності, наприклад, темпів зростання Національного внутрішнього продукту є більш актуальною, ніж значний його приріст, що не враховує реальний рівень Національного споживання і обмежені можливості зростання експорту. Тому при формуванні системи заходів необхідно враховувати як економічне становище держави, так і його місце в міжнародному поділі праці.

Ґрунтуючись на запропонованої моделі забезпечення економічної безпеки, має реалізовуватися у діяльності кожного суб'єкта. Однак той факт, що захищатися повинні економічні інтереси і між ними існують протиріччя, визначає необхідність розгляду особливості цього процесу.

**2. Механізми забезпечення безпеки соціальної системи - організації, сутність і завдання.**

Забезпечення безпеки є умовою існування і розвитку соціальної системи, що і дозволяє їй зберігати і примножувати вкладені кошти. Науковим критерієм забезпечення безпеки соціальної системи може служити значення рівня реалізації і захищеності інтересів.

Під забезпеченням безпеки організації розуміють цілеспрямовану діяльність керівництва організації та її структурних підрозділів, громадських інститутів, а також громадян з виявлення, попередження загроз безпеки організації та її персоналу. Характер цієї діяльності витікає з системи безпеки, визначається дотриманням принципів і політикою забезпечення безпеки, формульованій вищим керівництвом.

До числа основних принципів забезпечення безпеки організації зараховують законність, дотримання Конституції і законодавства країни щодо забезпечення безпеки, дотримання балансу життєво-важливих інтересів працівників, підприємства і держави, взаємна відповідальність підприємства із забезпечення безпеки.

Досягнення довгострокових цілей політики безпеки організації реалізується шляхом інтегрованості в систему стратегічного менеджменту підприємства, систему стратегічного планування у всіх сферах діяльності підприємства. Для ефективного здійснення політики безпеки, підприємством розробляється комплекс адміністративно-правових, організаційно-управлінських, спеціальних, інженерно-технічних, морально-психологічних, інформаційно-аналітичних тощо, заходів, спрямованих на вирішення завдань захисту функції розвитку організації.

Забезпечення безпеки соціальної системи - це основа буття, що випливає із діалектичного єдності функцій розвитку та безпеки. Якщо цільової функцією системи забезпечення безпеки є ступінь захищеності інтересів від загроз, то головною метою діяльності із забезпечення безпеки організації є комплексне нейтралізуючий вплив на потенційні і реальні загрози життєдіяльності організації, захист життєво важливих інтересів організації, інтересів добробуту, що виражають функцію існування та розвитку.

Дана мета досягається шляхом вирішення цілої низки завдань, що випливають з концепції безпеки та що визначаються керівництвом організації. Спектр цих завдань дуже широкий, але реально обмежується ресурсними можливостями підприємства. Він включає завдання забезпечення безпеки в основних сферах діяльності підприємства (технічної, комерційної, фінансової, захисної, бухгалтерської, адміністративно-управлінської), завдання, які повинні сприяти забезпеченню безпеки організації, а також завдання з планування та контролю діяльності підрозділів та сил безпеки в різних режимах їх функціонування.

Безпека організації - це єдина система видів безпеки, де під виглядом безпеки розуміється захист життєво важливих інтересів організації від загроз даного виду. Тому під забезпеченням безпеки організації слід завжди розуміти систему, що складається з низки підсистем. Кількість видів безпеки може бути будь-яка, але частіше обмежуються 8-10, основними видами є (економічна безпека, правова, маркетингова, інформаційна безпека, безпека фінансово-кредитної сфери, фізична, кадрова, особиста безпека, екологічна безпека, безпека в техногенної сфері та ін.). Реалізація цих видів безпеки спрямована на захист життєво-важливих корпоративних інтересів у різних сферах діяльності від внутрішніх та зовнішніх загроз і є обов'язковою умовою успіху в бізнесі, досягнення цілей, отримання прибутку і збереження цілісності підприємницької організаційної структури.

До об'єктів організації, таким, що підлягає обов'язковому захисту від потенціальних загроз і протиправних посягань, належать:

• персонал (керівники і персонал, який володіє інформацією, працівники зовнішніх служб тощо);

• фінансові кошти (валюта, дорогоцінні метали, фінансові документи);

• маткошти і ресурси (будівлі, споруди, сховища, обладнання, сировина, готова продукція тощо);

• інформаційні ресурси з обмеженим доступом, бази даних, програмне забезпечення;

• засоби і системи інформатизації;

• технічні засоби та системи охорони та захисту матеріальних та інформаційних ресурсів.

У самому загальному вигляді основні завдання у сфері безпеки підприємства можна визначити, як здійснення заходів за вказаними напрямками. Важливим моментом у системі безпеки є вибір механізмів забезпечення безпеки соціальної організації.

Коли в країні все є державним (переважає Державна власність), то абсолютно природно, що безпека господарюючого суб'єкта (організацій, підприємств) забезпечується державою, тобто держава повністю бере на себе захист його інтересів. В ринкових умовах господарювання ситуація докорінно змінюється. Частка держави в економіці та в інших сферах життя людини і суспільства безперервно скорочується, як і скорочується участь держави у забезпеченні безпеки особистості і суспільства. Тому в цих умовах захист інтересів організації та особистості не може бути тільки державної турботою, і об'єктивно виникає необхідність задіяння двох механізмів забезпечення безпеки – державний і недержавної.

Включення в безпеку соціальної системи - організації механізмів державної і недержавної систем забезпечення безпеки, означає по суті два важливих положення.

Перше пов'язано з тим, що діяльність соціальної організації (господарюючого суб'єкта) знаходиться в правовому полі, визначеній законодавством держави.

Друге, що безпека соціальної організації не може існувати сама пособі і органічно вписується в єдину державну політику забезпечення Національної безпеки в її конкретних видах, що розширює можливості забезпечення безпеки особистості і суспільства, через діяльність державних і недержавних структур безпеки.

При вивченні проблем безпеки організації важливе значення набуває її структурна класифікація.

На сьогоднішній день, в умовах глобалізації економіки, межу між внутрішньої і зовнішньої безпекою вельми розмита, а багато загрози - терористичні акти, захоплення заручників, екологічні та природні катастрофи - часом важко прив 'язати до якогось єдиного источнику. Тим не менш, ділення загроз на зовнішні і внутрішні представляється досить корисним з практичної точки зору, оскільки, воно дозволяє чітко класифікувати ті чи інші концептуальні підходи до розв 'язання проблем забезпечення безпеки організації.

Крім того, розподіл на внутрішню і зовнішню безпеку необхідно і для усвідомлення того, що при забезпеченні внутрішньої безпеки потрібні зовсім інші методи, форми і способи, ніж при забезпеченні зовнішньої безпеки. Основні напрями забезпечення внутрішньої безпеки соціальної системи (організації) - це рішення наступних завдань:

• зниження гостроти соціальних протиріч;

• захист організаційної культури, національних духовних, інтелектуальних і культурних цінностей;

• зміцнення виробничого потенціалу;

• проведення збалансованої економічної і фінансової політики;

• досягнення оптимального співвідношення інтересів людей, інтересів організацій, інтересів суспільства і держави;

• захист життя і здоров'я людей, створення гідних умов для роботи та існування;

• захист життєво важливих інтересів, захист майна, ресурсів та власності;

• підвищення рівня освіти та ін.

Сам перелік завдань показує особливе значення внутрішньої складової в забезпеченні безпеки соціальної організації та її ролі у зміцненні єдиного економічного простору країни.

Забезпечення зовнішньої безпеки, тобто зовнішній контур безпеки соціальної системи складається з двох рівнів: загально планетарного (глобального) і державного (рівня ділового середовища). При аналізі зовнішнього контуру безпеки важливо мати на увазі загрози ЕКО логічного, радіаційного, епідеміологічного, кримінального, природного, правового, економічного порядку і т. п.

Будь-яка концепція забезпечення безпеки розробляється відповідно до конкретних історичних умов. Раніше кожне підприємство з опорою на державу обходилося переважно власними силами для попередження і зниження гостроти виникаючих конфліктів і погроз.

Світ настільки інтегрований, що неможливо звести забезпечення зовнішньої безпеки підприємництва до рамок національних кордонів. Тому розумним єдиним шляхом забезпечення зовнішньої безпеки підприємств і організацій конкретної країни є досягнення певного балансу своїх інтересів та ідентичних інтересів інших сторін, певного компромісу в рамках міжнародної безпеки.

Міжнародна безпека ґрунтується на дотриманні всіма державами загальновизнаних принципів і норм міжнародного права, що виключають вирішення спірних питань і розбіжностей між ними за допомогою сили чи загрози силою.

Крім виділення в структурі безпеки організації двох зазначених вище типів (підсистем) - внутрішньої і зовнішньої безпеки - важливе значення має її класифікація за видами безпеки, що сприяє виробленню більш конкретної політики і стратегії забезпечення безпеки організації.

Однак "чисті" види безпеки зустрічаються рідко, вони, як правило, корелюють між собою.

Загальноприйнято вважати, що основним видом безпеки організації є її економічна безпека, під якою розуміється захист життєво важливих економічних інтересів організації від внутрішніх і зовнішніх загроз Економічна безпека є обов'язковою умовою успіху в бізнесі, отримання прибутку та збереження в цілісності підприємницької організаційної структури.

Економічна безпека — це цілісний вигляд безпеки. Він декомпонується на складові частини: правову, маркетингову, інформаційну, фінансово-кредитну, фізичну, освітню та ін. Ці складові частини економічної безпеки, по суті є видами безпеки, такими, що відображають захист життєво важливих інтересів організації та особистості від загроз по сферах або областям діяльності. Всі види безпеки тісно пов'язані між собою й перебувають у діалектичній взаємодії.

3. **Теоретичні засади моделювання діяльності з реалізації державної економічної політики у сфері інновацій та інвестицій.**

Загальні Положення моделювання, розглянуті раніше стосовно до системи забезпечення економічної безпеки, при їх конкретизації у сфері управління інвестиційними та інноваційними процесами дозволяють визначити напрямки діяльності з урахуванням пріоритетних завдань та реальних загроз. В даному випадку об'єктом моделювання є діяльність органів державної влади та управління, суб'єктів господарювання з реалізації інноваційної та інвестиційної політики України.

Важливість такої діяльності є першочерговим завданням будь-якого суспільства та будь-який соціальної системи. Адже без підтримання належного рівня розвитку науки і техніки, неможливо гідний розвиток та забезпечення безпеки, а заодно і збереження досягнутих результатів розвитку.

Як зазначалося раніше, у відповідності з системним підходом, модель реалізації інноваційної та інвестиційної політики в якості своїх елементів повинна включати:

- цілі та завдання діяльності;

- суб'єктів діяльності;

- об'єкт діяльності та його основні особливості;

-загрози об'єкту діяльності (інноваційної та інвестиційної політики) та механізми їх реалізації.

- умови, в яких ця діяльність здійснюється (або особливості економічній, політичній та інших сфер діяльності держави, що роблять вплив на інноваційну та інвестиційну політику);

– форми, методи та засоби, що використовуються суб'єктами діяльності для досягнення своїх цілей і вирішення конкретних задач;

- стратегія і тактика використання економічних, правових, адміністративних, організаційних та інших форм, методів і засобів реалізації інноваційної та інвестиційної політики;

- результат діяльності як прогнозована форма досягнення мети, його показники, критерії досягнення.

Вихідним моментом моделювання є визначення цілі такої діяльності. На нашу думку, вона може формулюватися, з одного боку, в загальному плані як забезпечення сталого економічного зростання і в першу чергу нарощування експортного потенціалу, які можуть досягатися за рахунок інтенсивного розвитку високотехнологічних виробництв, як базових для всіх інших галузей промисловості, підвищення технологічного рівня та конкурентоспроможності продукції, заміщення імпорту на внутрішньому ринку продукцією вітчизняного виробництва. З іншого, виходячи зі співвідношення з метою діяльності системи щодо забезпечення економічної безпеки, перша мета виступає як одна зі складових у загальній системі захисту національних економічних інтересів. Відповідно, цілі в даному випадку співвідносяться як частина з цілим, і при реалізації однієї з них забезпечується втілення інший.

Визначення мети діяльності дозволяє спочатку формувати підходи до організації роботи кожного з суб 'єктів виходячи з оцінки стану економічної системи на даний момент часу, дозволяє ввести як би "якісний" критерій оцінки правильності зроблених дій і можливість їх співвіднесення з кінцевим результатом, тобто оцінити ефективність діяльності і ступінь досягнення результату. Тобто, має бути побудована модель реалізації інноваційної та інвестиційної політики, що дозволяє забезпечувати такий стан системи економічних відносин, яке дозволить за рахунок саме регуляції та використання зовнішніх факторів впливу забезпечити досягнення поставленої мети.

Одним з основоположних питань аналізу та побудови моделі діяльності з реалізації інноваційної та інвестиційної політики, що мають загальне значення, є, на нашу думку, проблема виокремлення "об'єкта" такої діяльності. На перший погляд може здатися, що відповідь лежить на поверхні - раз мова йде про інновації та інвестиції, то і об'єктом діяльності є їх реалізація у сфері економіки.

Однак, слід звернути увагу на те, що на всіх рівнях або держави, або підприємства, підходи до реалізації інноваційної та інвестиційної політики практично базуються на виокремлення в якості об'єкта тих чи інших проблем, вирішення яких є життєво-важливим економічним інтересом даного суб'єкта. Тобто, підприємство реалізує проблеми свого рівня, а держава - стратегію і тактику розвитку всієї економіки, з напрямком яких діяльність окремого суб'єкта (підприємства) може збігатися чи ні. Іншими словами, слід говорити про наявність фактично загального методологічного підходу до побудови навіть не моделі, а концепції інноваційної та інвестиційної політики і моделях її різнорівневої реалізації. В основі побудови рівневих моделей повинен лежати аналіз реально існуючих життєво-важливих економічних інтересів кожного суб'єкта і вплив на їхню діяльність різнопланових факторів. В залежності від цього повинні змінюватися форми і методи управлінського впливу, спрямовані на досягнення мети. Спільним для кожного рівня є націленість діяльності на забезпечення Національної економічної безпеки. В загальному плані економічні інтереси визначаються як сукупність потреб, що формуються у індивідів, соціальних спільностей та інших суб'єктів господарювання під впливом системи економічних відносин і що спонукають їх до активної господарської діяльності. Задоволення важливих, значущих потреб обумовлює процес функціонування й розвитку, як світової економіки, економік окремих країн, так і життєдіяльності окремого індивіда виробника. Стосовно до проблеми інноваційної та інвестиційної діяльності це означає, що розбіжність або суперечність інтересів, наприклад, держави та підприємства при реалізації стратегічної лінії може знизити ефективність останньої або через відсутність нормативно закріплених стимулів інвестування, або через пріоритетності на даному часовому відрізку інших завдань діяльності виробника. Іншими словами, тут піднімається завдання вироблення цілей інноваційної та інвестиційної політики в державі, що збігається з інтересами кожного виробника. Але крім цього, чітко акцентується увага на тому, що об'єктом інноваційної та інвестиційної діяльності є інтереси кожного з суб'єктів системи. Відповідно розв'язання суперечностей повинно і може бути досягнуто за рахунок прийняття управлінського рішення, що забезпечує взаємовигідні умови - для суб'єкта господарювання з реалізації його інтересів (наприклад, в отриманні максимальної прибутку від вдосконалення технології виробництва), а для держави - зміцнення економічної системи як однієї з складовою Національної економічної безпеки.

Не менш важливе методологічне значення для побудови моделі реалізації інноваційної та інвестиційної політики поряд з її об'єктом набуває питання про реальні та потенційні загрози об'єкту діяльності - інтересам, умовам і можливостям їх реалізації. Розробка моделі повинна ґрунтуватися на обліку всього комплексу загроз, а саме - що формуються умов і факторів, що негативно впливають на прогресивний розвиток країни, що перешкоджають або що виключають можливість реалізації стратегії і тактики інноваційної та інвестиційної політики.

Стосовно до нинішьої ситуації в державі, мову слід вести про співвідношення зовнішніх і внутрішніх загроз, обумовлених наявністю і загостренням протиріч як всередині держави, так і у відносинах з іншими державами.

Виключення процесів і факторів економічного розвитку, що становлять загрозу інноваційної та інвестиційної політиці або її реалізації суб'єктами господарювання, повинно базуватися на оцінці ступеня їхнього впливу на умови і можливості реалізації життєво важливих економічних інтересів. Наприклад, ряд зарубіжних економістів вважають однією з причин низької інвестиційної активності незавершеність процесів приватизації, відсутність гарантій збереження зарубіжних капіталів. У цьому зв'язку, мабуть, доцільно проводити більш детальну класифікацію факторів, процесів і дій, що становлять загрози інноваційним та інвестиційним процесам, що дозволить підійти до проблеми їхньої реалізації з урахуванням ситуації в країні.

Однією з підстав такої класифікації може стати виключення факторів, що впливають на реалізацію економічних інтересів. До другої групи факторів, на наш погляд, відносяться фактори, що забезпечують стійкість економічного розвитку. Третя група - фактори, що створюють умови для взаємовигідної (для держави і суб’ єкта господарювання) інноваційного або інвестиційного процесів. Мабуть, доцільно проводити класифікацію і з інших підстав. Така класифікація, на нашу думку, дозволить більш детально врахувати всі фактори при формуванні моделі реалізації інноваційної та інвестиційної політики, розмежувати компетенцію державних органів і сформулювати завдання з розроблення та реалізації стратегії і тактики на найближчу і віддалену перспективу.

Для побудови моделі реалізації інноваційної та інвестиційної політики методологічне значення також має й питання щодо визначенні "носіїв", джерел або суб'єктів загроз, чиї саме дії і спрямовані проти досягнення її результатів. Та якщо в одному разі їх носіями є об'єктивні процеси і фактори економічного розвитку, то в іншому, такими є конкретні суб'єкти господарювання.

В якості суб'єктів загроз реалізації інноваційної та інвестиційної політики, чиї конкретні дії завдають шкоди життєво - важливим економічним інтересам країни, можна, на наш погляд, розглядати:

- підприємців, фірми, фонди та благодійні організації; державні підприємства та інші суб'єкти господарювання, нецільовим чином які витрачають кошти, призначені на розвиток і реконструкцію виробництва;

- іноземні організації, фірми і т. д., що ставлять своєю метою використовувати ситуацію в Україні для реалізації найчастіше протиправних дій (наприклад, для відмивання незаконних доходів).

В цьому випадку мова повинна йти про створення таких умов регулювання економічних відносин, за яких суб'єкту господарювання невигідно використовувати інноваційні або інвестиційні ресурси не за цільовим призначенням.

У цьому зв'язку не менш важливо визначити співвідношення життєво-важливих економічних інтересів особи, суспільства і держави. В іншому випадку об'єктивно наявні суперечності між ними будуть ускладнювати діяльність держави з регулювання господарської практики: або будуть створювати штучні бар'єри у діяльності суб'єктів господарювання щодо впровадження нових технологій; або держава може втратити контроль і можливості чинити хоч яке-небудь позитивну реальну дію на економіку.

Таким чином, побудова моделі реалізації інноваційної та інвестиційної політики має, на наш погляд, базуватися на розглянутих методологічних підходах і включати створення системи що реалізує цю політику в діяльності кожного суб'єкта господарювання.

Для відтворення сцени для різних рівнів реалізації інноваційної та інвестиційної політики необхідно на сучасному етапі реалізувати низку заходів, метою яких є облік національних особливостей України і встановлення сприятливих умов їх реалізації.

**Висновок.**

При виконанні робіт можна використовувати певну модель системи інформаційної безпеки побудовану відповідно до стандарту (ISO 15408) і даних аналізу ризиків (ISO 17799). Ця модель відповідає спеціальним нормативним документам із гарантування інформаційної безпеки, прийнятих в Україні, міжнародному стандарту ISO/IEC 15408 "Інформаційна технологія - методи захисту, критерії оцінки інформаційної безпеки", стандарту ISO/IEC 17799 "Управління інформаційною безпекою" і враховує тенденції розвитку вітчизняної нормативної бази з питань інформаційної безпеки.

Об'єктивні чинники моделі:

* загрози інформаційній безпеці, що характеризуються вірогідністю реалізації;
* вразливі місця інформаційної системи або системи контрзаходів (системи інформаційної безпеки);
* ризик - чинник, що відображує можливий збиток організації в результаті реалізації загрози інформаційної безпеки: просочування інформації та її неправомірного використання (ризик відображає вірогідні фінансові втрати - прямі або непрямі).

Для побудови збалансованої системи інформаційної безпеки потрібно спочатку провести аналіз ризиків у сфері інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику.

**Завдання для самостійної роботи**

1. Яке визначення поняття «економічна безпека підприємства» є найбільш комплексним?

2. Визначення категоріального апарату дисципліни.

3. Якими концептуальними положеннями управління економічною безпекою підприємства ви б доповнили поданий перелік?

4. Які елементи світового досвіду забезпечення економічної безпеки підприємства доцільно запровадити в Україні та як їх адаптувати під особливості ведення вітчизняного бізнесу?

**Питання для самоконтролю**

1. Об'єктивні чинники моделі

2. Принципами побудови збалансованої системи інформаційної безпеки підприємства є?

3. Назвіть перелік вимог до системи інформаційної безпеки

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Вітлінський, В. В. Ризикологія в економіці та підприємництві [Текст] / В. В. Вітлінський, Г. І. Великоіваненко. – К.: КНЕУ, 2004. – 480 с.

2. Завгородний, В. И. Системный анализ информационных рисков [Текст]/ В. И. Завгородний // Вестник Финансовой академии. № 4, 2008. – С. 102–109.

3. 3егжда, П. Д. Теория и практика обеспечения информационной безо­пасности [Текст] / П. Д. Зегжда. – М.: Яхтсмен, 1996. – 192 с.

4. Клименюк, М. М. Управління ризиками в економіці: Навч. посіб. для студ. вищ. навч. закл. [Текст] / М. М. Клименюк, І. А. Брижань; Акад. муніцип. упр. – К., 2000. – 253 с.

5. Ортинський, В. Л. Економічна безпека підприємств, організацій та установ [Електронний ресурс] /В. Л. Ортинський // Модель побудови системи інформаційної безпеки. – Режим доступу: http://westudents.com.ua/glavy/16530-model-pobudovi-sistemi-nformatsyno-bezpeki.html

**Лекція №9**

**Тема. Антикорупційна політика компанії**

**Мета:** визначення поняття корупції, причини та наслідки корупції. Вивчення основних антикорупційних документів компанії.

**План**

1. Антикорупційна політика як функція держави

2. Визначення і зміст антикорупційної політики

3. Антикорупційні документи компанії

4. Підприємства, для яких затвердження антикорупційної програми є обов’язковим

5. Антикорупційна програма підприємства, порядок узгодження, затвердження та доведення до відома працівників

6. Зміст та структура антикорупційної програми

**Вступ**

В українській політологічній енциклопедії корупція (від лат. Corrumpere — псувати) означає протиправну діяльність, яка полягає у використанні службовими особами їхніх прав і посадових можливостей для особистого збагачення; підкупність і продажність громадських і політичних діячів. Так само трактує термін «корупція» і Закон України «Про запобігання корупції», згідно якого, корупція – це використання посадовою особою, наданих їй службових повноважень чи пов’язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов’язаних з ними можливостей.

Натомість британська енциклопедія, вказує на те, що корупція є неправомірною і неправовою поведінкою особи, яка має на меті отримання вигоди однією особою за рахунок іншої. Вона існує за умов суспільної байдужості чи слабкості правоохоронних органів. У суспільствах, де дарування подарунків є певним ритуалом, розмежувальна лінія між тим, що прийнятно, а що ні, стирається.

Найчастіше термін застосовується стосовно бюрократичного апарату і політичної еліти. Характерною ознакою корупції є конфлікт між діями посадової особи та інтересами її працедавця або конфлікт між діями виборної особи й інтересами суспільства. Багато видів корупції аналогічні шахрайству, що здійснюється посадовою особою, і відносяться до категорії злочинів проти державної влади.

**1. Антикорупційна політика як функція держави**

Будь-яка держава має свої функції, які представляють собою основні завдання та напрямки його діяльності, тобто предметно конкретизують сенс держави як форми організації суспільства. Деякі з функцій держави, наприклад, функції оборони, національної безпеки, підтримки (охорони) громадського порядку - традиційні, оскільки необхідність саме їх здійснення послужила головною причиною зародження держави як історичної категорії. Вони і донині залишаються типовими для сучасної державності.

Хоча протягом століть змінювалося зміст цих функцій, самі вони навіть в глобалізованому світі зберігають своє значення. Є функції і відносно нові, що сформувалися в кінці XIX - початку XX ст. Такі, наприклад, соціальні функції - забезпечення обов'язковою освітою, безкоштовною охороною здоров'я, соціальне забезпечення та обов'язкове соціальне страхування, охорона природи та ін. Дані функції також стали досить типовими для сучасної державності. Не випадково в сучасній політичній (конституційно-правовій) мові закріпилося поняття "соціальна держава".

Залежно від історичних традицій, національних особливостей і суспільного ладу в тій чи іншій країні держава покладає на себе і інші функції. Наприклад, в СРСР безпосереднє господарювання, управління всіма економічними процесами та об'єктами становило монополію держави; настільки ж невід'ємною функцією було "комуністичне виховання"; в ряді країн існує функція охорони та підтримки домінуючою релігії (наприклад, у Греції) і т.д.

В даний час проблема оптимального пошуку функцій держави та обсягу їх змісту обговорюється досить активно, фактично йдеться про два полярні світогляди - максимально повного державного контролю і настільки ж максимально повного "відходу держави" навіть зі звичних публічних сфер. Зрозуміло, що в принципі обидва ці світогляди ведуть до катастрофічних наслідків. У першому випадку - до тоталітаризму, у другому - до хаосу, а через нього - до диктатури. Але нас у даному випадку цікавить лише сам факт таких дискусій, які означають в якійсь мірі незадоволеність постінду-стріального суспільства деякими тенденціями цивілізаційної властивості.

Одна з таких тенденцій - коррумпування державного апарату. Дотепер поширена думка, що масштабна, системна корупція - властивість перехідних і слаборозвинених країн. Дійсно, в країнах з розвиненою ринковою економікою та усталеними демократичними інститутами ступінь корупції менше і в них порівняно невелика "низова", або побутова корупція, яка зазвичай найбільш яскраво демонструє розкладання державного апарату.

Однак сьогодні вже жодна країна не може вважати себе "застрахованою" від корупції. Світ глобалізується, а отже, корупція стає вже не проблемою окремих країн, а планетарною проблемою. І ця тенденція поступово все більше усвідомлюється.

Можна додати до цього ще, як мінімум, три очевидних аргументи, які свідчать про небезпеку корупції для всіх, а не тільки слаборозвинених і перехідних країн.

Аргумент перший. Взаємозалежність економік, в т.ч. фінансових ринків розвинених і частково країн, що розвиваються, не тільки представляє собою певне благо, дозволяючи вільно переміщатися капіталам, товарам і послугам, але й істотно підвищує ризик обвального руйнування світової економічної системи в разі краху хоча б одного з великих ринків. Немає потреби говорити, що сьогодні ринок може зруйнуватися внаслідок підвищення рівня його корупційності. Іншими словами, глобалізація економіки несе з собою і глобалізацію корупції.

Аргумент другий. Однією з головних загроз окремим країнам і міжнародній безпеці став тероризм. Але тероризм успішний багато в чому завдяки саме дрібним і великим корупційним операціях. Як у терориста, так і у корупціонера "немає батьківщини". У них є тільки особисті цілі, хоча для терористів-організаторів ці цілі артикулюються як "ідейні".

Аргумент третій. Високий рівень корупції стає зручним приводом для політичних спекуляцій і легко приводить до влади сильного тоталітарного ладу. Зрозуміло, корупція в умовах диктатури і тотального контролю не зменшується, а тільки видозмінюється. Але, по-перше, усвідомлення суспільством масштабів корупції затушовується через закритість диктаторських режимів, а по-друге, навіть якщо таке усвідомлення виникає, воно не впливає на масштаби корупції, бо демократичні інститути вже не діють. Загроза встановлення подібних режимів небезпечна не тільки для самих перехідних країн, а й для їхніх сусідів, а також для всього світового співтовариства, бо нинішній устрій світового порядку, що включає, наприклад, поняття "країна-ізгой", істотно знижує рівень міжнародної безпеки.

Зрозуміло, сказане не означає, що багато держав - як розвинені, так і перехідні - не розуміють небезпек корупції. Мова йде лише про те, що комплекси захисних заходів від корупції відображають трохи застарілий погляд на корупцію тільки як на різновид злочинів або дисциплінарних проступків. Цей погляд шкідливий тим, що сповідуючи його, держава консервує традиційні антикорупційні стратегії - "свідомої пасивності" або "війни".

Загальнолюдський прогрес зумовив радикальне підвищення корупційної небезпеки для всього світу. Але досягнення прогресу здатні служити і для вибудовування системи захисту від негативних явищ і загроз. Нова реальність зобов'язує по-новому поглянути і на арсенал засобів, які може протиставити суспільство корупційної небезпеки.

Корупція без постійної протидії їй має властивість розширюватися. Ось чому все більш природним для будь-якої держави стає здійснення постійної антикорупційної політики. Лише ця стратегія видається єдино ефективною в нинішніх умовах. При цьому вона не протиставляється застосуванню правового державного примусу до корупціонерів. Навпаки, це примус стає більш ефективним, оскільки вбудовується в загальну систему антикорупційного стримування.

Зокрема, проводячи антикорупційну політику, держава і суспільство можуть побачити, в чому полягають слабкості поліцейського, контрольного та судового механізмів і скорегувати ці механізми, а головне - мінімізувати корупційні прояви в самих юрисдикційних органах.

Державна антикорупційна політика України (далі – антикорупційна політика) формується і реалізується за умов, коли у суспільстві нівелюється різниця між правомірною та неправомірною поведінкою через розповсюдження правового нігілізму в країні. Таке становище вимагає зростання ваги несилових (політичних, економічних, соціальних, енергетичних, екологічних, інформаційних тощо) складових забезпечення антикорупційної політики.

**1. Визначення і зміст антикорупційної політики**

Антикорупційна політика - це розробка і постійне здійснення різнобічних і послідовних заходів держави і суспільства в рамках прийнятих даними державою основ конституційного ладу з метою усунення причин і умов, що породжують і живлять корупцію в різних сферах життя.

Розробка антикорупційної політики починається зі з'ясування її основних напрямків. Ці напрямки властиві практично будь-якій державі, навіть такій, де рівень корупції в даний час не є загрозливим. Інша справа - зміст конкретних заходів, що укладаються в кожен з напрямків (блоків). Тут універсалізму бути не може. Більше того, зміст напрямків антикорупційної політики має коригуватися не тільки в міру здійснення окремих заходів, але і з урахуванням результатів глибинних досліджень корупції, заснованих на науковому підході, зокрема, після більш ретельного вивчення причин корупції.

Щоб краще зрозуміти те чи інше явище, той чи інший процес, необхідно розглянути, з яких складових частин, елементів дане явище (процес) складається. Особливо це відноситься до нових категорій, що вводиться в науковий і практичний оборот, яким є антикорупційна політика.

Елементи антикорупційної політики можна розбити за кількома критеріями.

*Тривалість антикорупційних заходів.*

За даним критерієм антикорупційна політика розбивається на разові і постійні заходи.

Разові заходи можуть здійснюватися в різних сегментах державного і суспільного життя. Вони народжуються в залежності від конкретного стану політичної системи даної держави, масштабів корупції, стану законодавства, рівня ефективності поліцейської та іншої юрисдикційної діяльності і т.д. Іншими словами, разові заходи завжди індивідуальні по відношенню до конкретної країни. У той же час зрозуміло, що вивчення їх ефективності впливає і на визначення постійних заходів, і на пошук нових (наступних) разових заходів, і на збагачення досвіду антикорупційної політики в інших країнах.

До разових заходах в сучасній Україні можна віднести, наприклад, такі як: законодавче приведення допустимого розміру виборчих фондів у відповідність з реальними витратами на виборчі кампанії; прийняття закону про лобіювання з метою створення прозорої системи відстоювання інтересів у законодавчих органах; введення кодифікованої системи процедур підготовки та прийняття адміністративних рішень, іншої адміністративної діяльності, пов'язаної з відносинами між держслужбовцями та фізичними і юридичними особами; завершення переведення обслуговування всіх рахунків Федерального бюджету в казначейство; ліквідація інституту "уповноважених банків".

Таким чином, конкретна разова міра зникає зі складу антикорупційної політики після того, як вона реалізована. Сам же факт реалізації разових заходів визначається за формальними підставами (зокрема, прийняття відповідного нормативного акта або завершення організаційної перебудови). Інша справа, якщо після прийняття, наприклад, якогось закону в якості разового заходу ситуація в даному сегменті корупції не змінюється.

У цьому випадку антикорупційна політика припускає, природно, аналіз причин неефективності і на цій основі - або корекцію відповідної міри, або відмова від неї і пошук іншої.

Постійні заходи включають в себе:

a) розробку на певний період самої антикорупційної програми, тобто документа, що містить основні напрямки політики на даний період;

б) розробку на певний період планів з протидії корупції, тобто документів, що конкретизують і структурують антикорупційну програму;

в) контроль за реалізацією антикорупційної програми і планів з внесенням до них необхідних коректив і оцінка ступеня їх реалізованості;

г) діяльність спеціалізованого антикорупційного органу з протидії корупції (якщо такий створений);

д) діяльність правоохоронних органів щодо виявлення, припинення та розслідування фактів корупції;

е) судову практику в частині застосування відповідальності за корупційні діяння;

ж) діяльність контролюючих інстанцій (контрольно-ревізійних комісій по парламентським розслідуванням і ін.);

з) моніторинг стану корупції (в територіальному, галузевому і функціональному розрізах), у тому числі за допомогою статистичних, соціологічних та інших методів;

і) моніторинг системи інститутів влади з точки зору їх ефективності в протидії корупції;

к) антикорупційне освіта і виховання.

Постійні заходи, як неважко помітити, є заходами, універсальними для різних держав, тобто не залежать від масштабів корупції, політичного та економічного устрою.

*Стадії антикорупційної політики.*

Мова йде про послідовності основних кроків і змісті методів даної політики. За цим критерієм антикорупційну політику можна розбити на наступні групи:

а) розробка антикорупційних програм,

б) планування антикорупційних заходів;

в) прогнозування та аналіз стану корупції і тенденцій в її розвитку;

г) розробка спеціальних антикорупційних законопроектів і проектів підзаконних актів;

д) експертиза законопроектів і проектів підзаконних актів;

е) моніторинг реалізації антикорупційної політики та стану корупції;

ж) звітність державних органів для оцінки ефективності їх антикорупційної діяльності.

*Напрями антикорупційної політики.*

Класифікація, побудована за даним критерієм, є стрижневою, оскільки дозволяє оцінити, наскільки адекватно держава розуміє, що саме необхідно міняти у своєму апараті та функціонуванні для зменшення масштабів корупції. Основними напрямками антикорупційної політики є:

- корекція законодавства;

- більш збалансована система стримувань і противаг між основними інститутами влади;

- упорядкування системи, структури і функцій органів виконавчої влади;

- зміна принципів державної (насамперед, публічної цивільної) служби і контроль за майновим становищем представників влади;

- створення умов для ефективного контролю за розподілом і витрачанням бюджетних коштів;

- зміцнення судової влади;

- вдосконалення правоохоронної системи і поліцейської діяльності (діяльності спецслужб);

- координація антикорупційної політики.

**3. Антикорупційні документи компан**і**ї**

Загальнодержавний тренд боротьби з корупцією сьогодні набирає все більше обертів. Законом України «Про запобігання корупції» (далі – Закон) передбачено, що на підприємствах повинна діяти низка локальних антикорупційних документів, проте далеко не всі суб’єкти знають про це та дотримуються вимог. Тому варто розібратися в особливостях антикорупційної документації, наявність якої є обов’язковою для більшості господарюючих суб’єктів.

1. Антикорупційна програма (ст. 62 Закону) – своєрідний механізм боротьби з корупцією в діяльності юридичної особи через відповідні правила та процедури. Така програма розробляється з урахуванням особливостей конкретного підприємства (організаційно-правової форми, чисельності працівників, сфери діяльності, тощо).

Серед приватних суб’єктів розробити та затвердити на своєму підприємстві Антикорупційну програму повинні юридичні особи – учасники закупівель, де вартість товару, послуг, робіт більша або дорівнює 20 мільйонам гривень.

Наявність Антикорупційної програми також є обов’язковою для ДП та КП, господарських товариств із державною/комунальною часткою більше ніж 50%, в яких у середньому працює більше ніж 50 осіб, а дохід від реалізації – більше 70 мільйонів гривень.

Згідно з нормами антикорупційного законодавства типова форма Антикорупційної програми має бути розроблена та затверджена Національним агентством з питань запобігання корупції, але станом на сьогодні цього не відбулося. Тому всі, хто підпадає під дію Закону, самостійно «рухаються» у цьому напрямку – зокрема, чимало електронних ресурсів у вільному доступі пропонують зразки таким програм.

Але, аналізуючи практику публічних закупівель, де антикорупційна програма є обов’язковим документом для учасника, можна сказати, що замовники торгів прискіпливо вивчають цей документ, звертаючи увагу на подібність за текстом поданих антикорупційних програм, мотивують відмову у прийнятті тендерних пропозицій «попередньою змовою учасників». Отже, до питання розроблення та затвердження антикорупційної програми кожне підприємство (установа, організація) має підійти відповідально та професійно.

Вимоги щодо змісту антикорупційної програми юридичної особи визначено статтею 63 Закону, в ній має передбачатись: опис заходів для реалізації антикорупційної стратегії на підприємстві, перелік заходів щодо запобігання виникненню конфлікту інтересів і шляхи їх вирішення, якщо має місце виникнення таких, відповідальність за порушення вимог програми, заборону використання працівниками своїх посадових повноважень з корисливою метою для себе чи інших осіб та конкретні практичні рекомендації, які підприємство (установа, організація) впроваджує для запобігання корупції у своїй діяльності.

Проект антикорупційної програми підлягає погодженню з працівниками юридичної особи. Лише після цього керівник своїм наказом затверджує програму. Норму про обов’язковість виконання програми слід включити до правил внутрішнього розпорядку, трудових договорів, а також – можна додати до договорів із контрагентами.

1. Наказ про призначення та положення про уповноважену особу з питань запобігання корупції.

Наступним кроком, який тісно пов’язаний із створенням антикорупційної програми, є призначення уповноваженої особи з питань запобігання корупції (ст. 64 Закону). Адже саме для втілення в життя антикорупційної програми Законом передбачено призначення особи, відповідальної за її реалізацію. Отже, наступний антикорупційний документ, який необхідно розробити – це наказ про призначення такої особи та положення про неї.

Порядок призначення уповноваженої особи повинен бути визначений у самій антикорупційній програмі. Такою особою, відповідно до Закону, може бути фізична особа, з числа працівників підприємства, що володіє достатнім професійним рівнем, моральними якостями, станом здоров’я. Ні стажу роботи в галузі права, ні вищої юридичної освіти для зайняття цієї посади тепер не потрібно.

Аби належним чином врегулювати права та обов’язки Уповноваженого саме на даному підприємстві, бажано затвердити локальне положення про нього.

Відсутність антикорупційних документів на підприємстві може стати підставою для притягнення до відповідальності керівника такого підприємства та/або відповідального за протидію корупції, а саме:

• адміністративної відповідальності у вигляді штрафу за невжиття заходів щодо протидії корупції (застосовується у разі виявлення корупційного правопорушення), становить від 2040 до 6800 гривень;

• кримінальної відповідальності у вигляді таких альтернативних покарань: штраф до 8500 гривень, виправні роботи строком до 2 років, обмеження волі строком до 3 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років.

Також передбачена неможливість участі у процедурах закупівлі.

3. Порядок використання електронного цифрового підпису.

Законодавством передбачено додатковий механізм протидії корупції, а саме: використання як юридичними, так і фізичними особами у своїй діяльності електронного цифрового підпису (далі – ЕЦП). Перш за все, ЕЦП є необхідною передумовою для подання електронних декларацій. Окрім того, сучасні інформаційні технології дають можливість більш ефективно (безпаперово) вирішувати економічні та соціальні питання через електронний документообіг. ЕЦП підтверджує авторство документа, в той же час надійно захищаючи його від можливої фальсифікації.

Використання ЕЦП на підприємстві (установі, організації) врегульовується наказом керівника. Зокрема, йому необхідно створити спеціальний підрозділ чи призначити працівника, який буде наділений відповідними повноваженнями щодо забезпечення здійснення електронного документообігу на підприємстві, підготовки та подання необхідної інформації до центру сертифікації ключів, ведення обліку засобів ЕЦП та носіїв особистих ключів підписувача електронних документів, схоронності документів та їх копій, за якими було отримано відповідні послуги, контролю за діяльністю підписувачів електронних документів, тощо.

Порядок використання ЕЦП на підприємстві (установі, організації) має бути передбачений відповідним положенням, яке затверджується наказом керівника та поширюється на всіх працівників, які використовують ЕЦП під час виконання своїх службових обов’язків.

За загальним правилом, відповідальність за те, як буде організовано електронний документообіг, несе керівник юридичної особи.

4. Кодекс чи стандарт етичної поведінки (для державних підприємств, державних органів, органів місцевого самоврядування) – у випадку необхідності (ст. 37 Закону).

Законом передбачено можливість розробки галузевих кодексів чи стандартів етичної поведінки держорганами та органами місцевого самоврядування для своїх працівників. Це не є обовя’зковою вимогою, проте цілком доцільно для тих міст, громад, які прагнуть до розвитку та вдосконалення свого іміджу.

**4. Підприємства, для яких затвердження антикорупційної програми є обов’язковим.**

Українське антикорупційне законодавство передбачає обов’язок запровадження антикорупційної програми для юридичних осіб приватного права, які є учасниками попередньої кваліфікації, учасниками процедури закупівлі відповідно до Закону України "Про здійснення державних закупівель", якщо вартість закупівлі товару (товарів), послуги (послуг) дорівнює або перевищує 1 мільйон гривень, а робіт – 5 мільйонів гривень.

Однак, мати антикорупційну програму доцільно й іншим категоріям підприємств з метою уникнення ризику накладення кримінально-правових санкцій на підприємство через недотримання його уповноваженими особами вимог щодо запобігання та протидії корупції на підприємстві, що передбачені Кримінальним кодексом України. Тому, питання розробки та впровадження антикорупційної програми є актуальним для всіх підприємств.

**5. Антикорупційна програма підприємства, порядок узгодження, затвердження та доведення до відома працівників.**

Антикорупційну програму слід викладати у формі окремого письмового документу, що затверджується відповідним наказом керівника підприємства. Законодавство встановлює наступні обов’язкові вимоги до антикорупційної програми підприємства:

1. Антикорупційна програма має затверджуватися лише після її обговорення з працівниками підприємства. Законодавство не встановлює обов’язкової форми такого "обговорення", проте доцільною формою ввижається проведення загальних зборів трудового колективу з цього приводу. Рекомендується попередньо надати проект для ознайомлення (в друкованому чи електронному вигляді), та з наступним затвердженням проекту на загальних зборах трудового колективу, тощо.

2. Текст антикорупційної програми повинен постійно перебувати у відкритому доступі для працівників підприємства. Така вимога може бути реалізована шляхом розміщення тексту програми на внутрішньому корпоративному сайті підприємства чи фізичного розміщення друкованого тексту в конкретному місці (на дошці оголошень). Важливо, щоб спосіб, у який працівник може ознайомитися зі змістом антикорупційної програми, вказувався у трудовому договорі, посадовій інструкції чи правилах внутрішнього трудового розпорядку. Окрім того, підприємствам рекомендується ознайомлювати працівників зі змістом антикорупційної програми під розпис і зберігати такий документ.

3. Положення щодо обов’язковості дотримання антикорупційної програми повинні бути включені до трудових договорів чи правил внутрішнього трудового розпорядку підприємства. Також, вони можуть включатися у договори, які укладаються юридичною особою (наприклад, цивільно-правові договори з окремими особами та господарські договори із контрагентами).

4. Для реалізації вимог антикорупційної програми на підприємствах, для яких створення антикорупційної програми є обов’язковим, має призначатися особа, відповідальна за реалізацію антикорупційної програми.

**6. Зміст та структура антикорупційної програми.**

Українське законодавство не передбачає вичерпного переліку питань, що мають бути обов’язкового висвітлені в антикорупційній програмі підприємства, однак вказує, що антикорупційна програма може містити наступні положення:

1) сферу застосування та коло осіб, на які поширюються її положення;

2) вичерпний перелік та опис антикорупційних заходів, стандартів, процедур та порядок їх виконання (застосування), зокрема порядок проведення періодичної оцінки корупційних ризиків у діяльності підприємства;

3) норми професійної етики працівників підприємства;

4) права та обов’язки працівників та засновників (учасників) підприємства щодо запобігання і протидії корупції у діяльності підприємства;

5) права та обов’язки посадової особи, відповідальної за запобігання корупції, та підпорядкованих їй працівників (у разі їх наявності);

6) порядок регулярного звітування особи, відповідальної за запобігання корупції, перед засновниками (учасниками) підприємства;

7) порядок здійснення належного нагляду, контролю та моніторингу за дотриманням антикорупційної програми у діяльності підприємства, а також оцінки результатів здійснення передбачених нею заходів;

8) умови конфіденційності інформування особи, відповідальної за запобігання корупції, працівниками про факти підбурювання їх до вчинення корупційного правопорушення або про вчинені іншими працівниками чи особами корупційних або пов’язаних з корупцією правопорушень;

9) процедури захисту працівників, які надали інформацію про корупційне або пов’язане з корупцією правопорушення;

10) процедуру інформування працівниками особи, відповідальної за запобігання корупції, про виникнення реального, потенційного конфлікту інтересів, а також порядок врегулювання виявленого конфлікту інтересів;

11) порядок проведення індивідуального консультування особи, відповідальної за запобігання корупції, працівників підприємства з питань застосування антикорупційних стандартів та процедур;

12) порядок проведення періодичного підвищення кваліфікації працівників у сфері запобігання та протидії корупції;

13) застосування заходів дисциплінарної відповідальності до працівників, які порушують положення антикорупційної програми;

14) порядок вжиття заходів реагування щодо виявлених фактів корупційних або пов’язаних з корупцією правопорушень, зокрема, інформування уповноважених державних органів, проведення внутрішніх розслідувань;

15) порядок внесення змін до антикорупційної програми.

Антикорупційноа програма зазвичай містить:

1) Перелік працівників, на яких розповсюджується дія антикорупційної програми.

2) Відомості про результати обговорення проекту антикорупційної програми з працівниками підприємства (з посиланням на дату проведення такого обговорення та на рішення, винесене в результаті такого обговорення (реквізити рішення, протоколу зборів, тощо).

3) Посилання на інші внутрішні документи підприємства у сфері запобігання та протидії корупції (карту корупційних ризиків у діяльності підприємства, положення про конфлікт інтересів та ін.), що існують у формі окремих документів чи додатків до антикорупційної програми.

4) Зазначення обов’язковості дотримання вимог такої антикорупційної програми для працівників.

5) Викладення основних положень антикорупційної програми.

6) Порядок призначення, вимоги до особи, відповідальної за реалізацію антикорупційної програми, її повноваження та обов'язки.

7) Порядок ознайомлення працівників зі змістом антикорупційної програми та отримання підтверджень про факт такого ознайомлення; положення про загальнодоступність тексту програми для працівників.

8) Порядок внесення змін до антикорупційної програми.

Підприємства при підготовці антикорупційної програми можуть виявляти гнучкість щодо формування змісту та структури антикорупційної програми, однак зазначені вище відомості рекомендується зазначати обовязково.

На підприємствах, для яких створення антикорупційної програми є обов'язковим, має бути призначена особа, відповідальна за реалізацію антикорупційної програми ("Уповноважений"), тобто, комплаєнс-спеціаліст.

Згідно з українським законодавством, Уповноважений має бути окремою посадовою особою підприємства, що призначається відповідно до законодавства про працю керівником підприємства або його учасниками (засновниками) у порядку, що передбачається антикорупційною програмою підприємства.

Обов’язки Уповноваженого та комплаєнс-спеціаліста підприємства є майже ідентичними.

Існування посади Уповноваженого, для окремих підприємств, є прямою законодавчою вимогою, тому вищевказаний порядок призначення Уповноваженого відповідно до вимог законодавства має бути повністю дотриманий таким підприємством.

Законом встановлені наступні вимоги до осіб, що можуть обіймати посаду Уповноваженого:

1. здатність за своїми діловими та моральними якостями, професійним рівнем, станом здоров’я виконувати відповідні обов’язки;

2. відсутність непогашеної чи незнятої судимості;

3. наявність повної дієздатності;

4. відповідність такої особи вимогам несумісності (з іншої діяльністю) та відсутність у неї реального чи потенційного конфлікту інтересів.

Окрім того, на посаду Уповноваженого не може бути призначена особа, яка була звільнена з посад у державних органах, органах місцевого самоврядування за порушення присяги або у зв’язку з вчиненням корупційного правопорушення чи правопорушення, пов’язаного з корупцією (протягом трьох років з дня такого звільнення).

У разі виникнення обставин несумісності посади Уповноваженого з іншою посадою, яку обіймає така особа, вона зобов’язана повідомити про це керівника підприємства у дводенний строк з дня виникнення таких обставин з одночасним поданням заяви про розірвання трудового договору за власною ініціативою.

Закон передбачає, що Уповноважений може бути звільнений з посади достроково у наступних випадках:

1) розірвання трудового договору з ініціативи Уповноваженого;

2) розірвання трудового договору з ініціативи керівника юридичної особи або її засновників (учасників);

3) неможливості виконання своїх повноважень за станом здоров’я відповідно до висновку медичної комісії, що створюється за рішенням спеціально уповноваженого центрального органу виконавчої влади, який реалізує державну політику у сфері охорони здоров’я;

4) набрання законної сили рішенням суду про визнання його недієздатним або обмеження його цивільної дієздатності, визнання його безвісно відсутнім чи оголошення його померлим;

5) набрання законної сили обвинувальним вироком суду щодо нього;

6) смерті.

На підприємствах, для яких законом передбачена обов’язковість прийняття антикорупційної програми та створення посади Уповноваженого, особа, яка перебуває на посаді Уповноваженого, може бути звільнена за ініціативи керівника підприємства лише за умови надання відповідної згоди Національним агентством з питань запобігання корупції. У разі звільнення особи з посади Уповноваженого на такому підприємстві з інших підстав, керівник підприємства зобов’язаний письмово повідомити Національне агентство з питань запобігання корупції протягом двох робочих днів та забезпечити невідкладне подання нової кандидатури на цю посаду.

Повноваження та обов’язки Уповноваженого мають обов’язково вказуватися в антикорупційні програмі, у трудовому договорі Уповноваженого з підприємством та його посадовій інструкції.

**Висновок.**

Антикорупційна політика - це розробка і постійне здійснення різнобічних і послідовних заходів держави і суспільства в рамках прийнятих даними державою основ конституційного ладу з метою усунення причин і умов, що породжують і живлять корупцію в різних сферах життя.

На підприємствах, для яких законом передбачена обов’язковість прийняття антикорупційної програми та створення посади Уповноваженого, особа, яка перебуває на посаді Уповноваженого, може бути звільнена за ініціативи керівника підприємства лише за умови надання відповідної згоди Національним агентством з питань запобігання корупції. У разі звільнення особи з посади Уповноваженого на такому підприємстві з інших підстав, керівник підприємства зобов’язаний письмово повідомити Національне агентство з питань запобігання корупції протягом двох робочих днів та забезпечити невідкладне подання нової кандидатури на цю посаду.

**Завдання для самостійної роботи**

Умова

Необхідно сформувати систему показників для проведення оцінки техніко-технологічної складової економічної безпеки підприємства, яке випускає залізобетонні конструкції.

Студент повинен визначити рівень техніко-технологічної складової та економічних параметрів економічної безпеки підприємства.

Необхідно запропонувати комплекс заходів для підвищення рівня економічної безпеки підприємства.

**Питання для самоконтролю**

1. Дайте визначення поняттю корупція

2. Назвіть причини та наслідки корупції

3. Особливості антикорупційної документації

4. Зміст та структура антикорупційної програми

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Конституція України. – К., 2015.

2. Конвенція ООН проти корупції (ратифікована Законом України від 18 жовтня 2006 р.) //Офіційний вісник України. – 2010. - №10/2006. - №44. – Ст.2938/

3. Кримінальна конвенція Ради Європи про боротьбу з корупцією (ратифікована Законом України від 18 жовтня 2006., №252 //Офіційний вісник. – 2006. - №9. – Ст.592. –С.252)

4. Лімська декларація. VIII Міжнародна конференція по боротьбі з корупцією 7-11 вересня 1997 р. //zakon3.rada.gov.ua

5. Закон України «Про запобігання корупції» від 14.10.2014 р. // Урядовий кур’єр. –05.11.2014 р. (зі змінами).

6. Закон України «Про Національне антикорупційне бюро України» від 14 жовтня 2014 р. //zakon.rada.gov.ua

**Лекція №10**

**Тема. Кадрова безпека компанії.**

**Мета:**  визначення кадрової безпеки, як однієї із найважливіших складових економічної безпеки, та систематизації наукових праць зарубіжних та вітчизняних вчених і практиків з питань кадрової безпеки та дослідження й розкриття суті, змісту та основних складових кадрової безпеки.

**План**

1. Визначення поняття кадрової безпеки

2. Об'єкти та суб’єкти кадрової безпеки.

3. Класифікація суб’єктів кадрової безпеки

4. Управління кадровими ризиками

**Вступ**

Сучасне підприємство можна розглядати, як складну систему, у якій взаємодіють матеріально – речовинна, інтелектуально – інноваційна та людська складова розвитку власної діяльності. Ефективне їхнє використання забезпечує режим економічної безпеки – це стабільне функціонування фірми, її динамічний науково-технічний і соціальний розвиток, запобігання внутрішнім і зовнішнім негативним впливам. Одною з найголовніших складових економічної безпеки підприємства, установи, організації вважається кадрова безпека. Співробітники впливають на всі аспекти життєдіяльності фірми, вони невід’ємно пов'язані з її ефективною діяльністю. Основною метою даної роботи є визначення поняття «кадрова безпека» та розкриття її основних складових частин.

Поняття «кадрова безпека» визначається, як комплекс дій та взаємовідношень персоналу, при якому відбувається ефективне економічне функціонування підприємства, його здатність протистояти внутрішнім і зовнішнім впливам і загрозам, пов’язаним з персоналом, діагностика та прогнозування впливу персоналу на показники роботи, його інтелектуальний потенціал і трудові відносини загалом. Кадрова безпека є синтетичною категорією: економічної теорії, теорії управління персоналом, економіки праці, соціології, політології.

**1. Визначення поняття кадрової безпеки**

Кадрова безпека була й залишається поняттям складним і багатогранним, тому вітчизняні та зарубіжні автори виокремлюють різні підходи до визначення поняття та розуміння сутності і змісту трактування категорії «кадрова безпека».

О. А. Кириченко [1] вважає, змістом категорії «кадрова безпека» правове та інформаційне забезпечення процесу управління персоналом: вирішення правових питань трудових відносин, підготовку нормативних документів, що їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом.

Отже, О. А. Кириченко визначає кадрову безпеку переважно з правового боку та з погляду соціально-трудових відносин та наголошує на репутаційній складовій.

Змістом категорії «кадрова безпека» на думку О. Лащенка,А. І. Маренича та Н. Г. Мехеди є характеристика стану економічної системи за якої відбувається ефективне функціонування всіх її функціональних складових, забезпечення захищеності та здатність протистоянь внутрішнім і зовнішнім впливам і загрозам пов’язаним з персоналом, змістовний та структурний аналіз, діагностика та прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники вказаної економічної системи. [2, 3].

Визначення кадрової безпеки, як системи, дав відомий фахівець з питань управління персоналом А. Кібанов. Він вважає, що кадрова безпека — «це генеральний напрямок кадрової роботи, сукупність принципів, методів, форм організаційного механізму з визначення цілей, завдань, спрямованих на збереження, зміцнення й розвиток кадрового потенціалу, на створення відповідального і високопродуктивного згуртованого колективу, здатного вчасно реагувати на постійно мінливі вимоги ринку з урахуванням стратегії розвитку організації» [4].

Отже, Кібанов розглядає кадрову безпеку як систему**,**тож можна зробити висновок, що складовими кадрової безпеки за Кібановим є:

- Соціально- мотиваційна безпека;

- Професійна безпека;

- Антиконфліктна (психологічна) безпека.

За І. Чумаріном «кадрова безпека — це процес запобігання негативним впливам на економічну безпеку підприємства за рахунок ризиків і загроз, пов’язаних із персоналом, його інтелектуальним потенціалом та трудовими відносинами в цілому». Подібний ризик орієнтований підхід, на думку авторки, є прогресивним й сучасним та потребує більшої деталізації. Розкриваючи зміст кадрової безпеки банківської установи, важливо охарактеризувати фактори впливу на неї. У своїй статті: «Що таке кадрова безпека компанії» І. Чумарін виокремлює три основні фактори, від яких залежить кадрова безпека будь-якого підприємства, а саме: найм, лояльність та контроль [5]***.*** Однак, як зауважують Л. А. Швайка та Х. В. Жидецької, ці фактори взаємопов’язані і при їх врахуванні діє принцип «компенсації недостатньої уваги» до попереднього фактору. Не застосування відповідних методів та прийомів щодо найму на роботу, без розвитку лояльності персоналу — останній фактор, тобто контроль вимагатиме найбільших ресурсів.

Систему економічної безпеки банку науковці та практики представляють комбінацією елементів, пов’язаних між собою різносторонніми зв’язками, що спрямовані на захист від загроз та протидію ним по найбільш важливих напрямках діяльності банку. У таблиці 1 наведені базові критерії системи показників економічної безпеки банку та базові критерії оцінки економічної безпеки.

Н. Логінова вважає, що саме кадрова безпека є найбільш важливою складовою економічної безпеки підприємства, яка має на меті виявлення, знешкодження, запобігання, відвернення та попередження загроз, небезпек і ризиків, які спрямовані на персонал та його інтелектуальний потенціал, і ті, які йдуть безпосередньо від нього, що повинно проявлятися в системі управління трудовими ресурсами та в кадровій політиці підприємства [6].

Більш орієнтований підхід до характеристики суті кадрової безпеки висловили С. Васильчак та І. Мацюняк, які вважають, що основною метою кадрової безпеки підприємства є не тільки запобігання та попередження негативних впливів від персоналу, а й захист самих працівників, створення сприятливих умов і стимулів для їх роботи. При цьому слід враховувати, що персонал — це виробничий ресурс, до якого на відміну від інших ресурсів потрібно застосовувати принцип гуманності та соціального захисту. Завданням служби безпеки є не тільки протидія негативному впливу, який йде від персоналу, а й протидія тим факторам, які спрямовані на нього [7].

О. Герсименко, Г. Козаченко, В. Пономарьов та О. Ляшенко визначають кадрову безпеку як процес запобігання негативним діям на безпеку підприємства за рахунок усунення ризиків і загроз, пов'язаних з інтелектуальним потенціалом та трудовими відносинами в цілому [8,9].

Проаналізувавши підходи до визначення поняття «кадрова безпека», запропоновано наступне визначення:

 Якщо розглядати кадрову безпеку в системі економічної безпеки як процес  - «Кадрова безпека - це процес моніторингу, мінімізації та превенції негативних впливів на економічну безпеку підприємства через ефективний ри­зик менеджмент загроз та небезпек, пов'язаних  з персоналом».

якщо розглядати систему кадрової безпеки підприємства як стан  -

 «Кадрова безпека – оптимальний стан захищеності персоналу від зовнішніх загроз та оптимальний стан економічної захищеностівід внутрішніх загроз з боку персоналу».

Для економічної безпеки велике значення мають не стільки самі показники, скільки їх порогові значення, тобто допустимі величини, недодержання яких буде перешкоджати оптимальному розвитку діяльності та бізнес процесам підприємства, зумовлювати формування негативних тенденцій його економічної безпеки.  Найвищий ступінь економічної безпеки підприємства досягається при умові, знаходження повного комплексу показників в рамках допустимих меж порогових значень, та порогові значення одного показника не досягається за рахунок іншого.

Дослідження практичних аспектів та наукових праць показало, що в основі управління кадровою безпекою на сьогодні чітко простежується ризик орієнтований підхід.

Оскільки робота з персоналом в будь-якому підприємства є первинною, тож кадрова безпека відіграє домінуючу роль у забезпеченні ефективної системи безпеки підприємства та мінімізації ризиків, що продукують кадри підприємства.

Ризики кадрової безпеки в банківських установах світу на сьогодні конвертуються в матеріальні та нематеріальні збитки та втрати, що проявляються зниженням корпоративної етики, втратою ділової репутації банківських установ, падінням вартості акцій і порушенням ділових відносин з партнерами.

Таблиця 1. Загальна типологія наслідків ризиків кадрової безпеки

|  |  |  |  |
| --- | --- | --- | --- |
| Ризики кадрової безпеки | | | |
| матеріальні збитки | | нематеріальні збитки | |
| падіння вартості акцій | порушення ділових відносин з партнерами | зниження корпоративної етики | втрата ділової репутації банківських установ |

**2. Об'єкти та суб’єкти кадрової безпеки.**

Оскільки кадри є первинними фактором для всіх функціональних складових економічної безпеки, проаналізувавши роботи науковців.

Таблиця 2. Об’єкти кадрової безпеки

|  |  |
| --- | --- |
| № п/п | Об’єкти кадрової безпеки |
| 1 | акціонери, керівники, партнери, штатний і позаштатний персонал, що володіє інформацією, яка не підлягає розголошенню або є комерційною таємницею; |
| 2 | фінансові ресурси, що знаходяться в розпорядженні персоналу банківської інституції та підпадають під можливість привласнення, розтрати й навмисні фінансові махінації; |
| 3 | технічні засоби та програмне забезпечення, що використовується співробітниками в процесі виконання їхніх посадових обов'язків, якому може бути завдано шкоди власним персоналом навмисно або ненавмисно; |
| 4 | об'єкти авторського права, об'єкти суміжних прав, об'єкти науково- технічної інформації, об'єкти банківської власності, засоби індивідуалізації, ноу-хау, що можуть стати об'єктами привласнення, розкрадання, махінацій, промислового шпіонажу і корпоративної розвідки, та навіть знищення власним персоналом; |
| 5 | усі матеріальні ресурси банківської інституції, до яких є вільний або обмежений доступ персоналу, що може вчинити такі неправомірні дії, як розкрадання майна, навмисне спричинення шкоди майну банка, тощо; |
| 6 | захищена інформація, інформаційні ресурси обмеженого використання та вільно розповсюджувані інформаційні ресурси, які є об'єктом захисту від несанкціонованого вилучення, збору й передачі третій, зацікавленій стороні, втраті, викривленню в інтересах зловмисника, розголошенню, що завдає шкоди інтересам та репутації підприємства. |

**3. Класифікація суб’єктів кадрової безпеки**

До зовнішніх відносяться: органи державної влади, правоохоронні органи, служби безпеки інших суб'єктів господарської діяльності, недержавні структури із забезпечення безпеки, особи, які не мають ділових відносин з банківською інституцією;

До внутрішніх відносяться: служба безпеки підприємства, кадрова служба, юридичний відділ, структурні підрозділи, персонал підприємства

Проаналізувавши наукові праці, можна виділити основні джерела загроз кадрової безпеки (рис. 1)

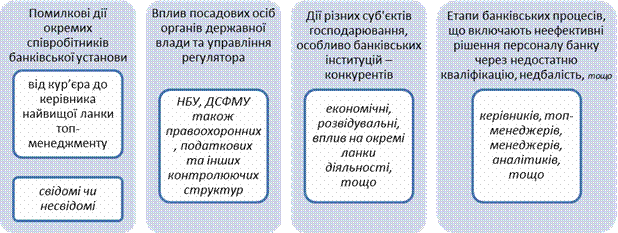


Рисунок 1. Джерела загроз кадрової безпеки

Кадрова безпека є комбінацією складових, пов’язаних між собою складними і часто багаторівневими процесними зв’язками. Кадрову безпеку підприємства можна досліджувати як комбінацію подібних складових.

Отже, персонал банківської установи як об’єкт управління характеризується професійною кваліфікацією, мотивацією та фізичною кондицією. Також банк є своєрідним осередком інформаційних даних, що акумулюються та обслуговуються персоналом підприємства. Потрібно пам’ятати, що дана структура – структура банківської інституції знаходиться у правовому полі України.

Подальше дослідження потребує аналітичної роботи стосовно ґрунтовного вивчення визначення вченими складових кадрової безпеки, що сформовано у вигляді таблиці 3.

Таблиця 3. Складові кадрової безпеки

|  |  |
| --- | --- |
| АВТОР | СИСТЕМА КАДРОВОЇ БЕЗПЕКИ |
| Кібанов А. Я. [4] | Психологічна безпека (антиконфліктна)  Соціально мотиваційна безпека  Професійна безпека |
| Томаневич Л. М. [10] | Безпека життєдіяльності  Психологічна безпека  Соціально мотиваційна безпека  Професійна безпека |
| Чередниченко Н. В. [11] | Безпека здоров’я  Фізична безпека  Фінансова безпека  Інтелектуальна безпека  Кар’єрна безпека  Адміністративно-незалежна  Технологічна безпека  Пенсійно-страхова безпека  Патріотична безпека  Психолого - комунікаційна  Естетична безпека |

Проаналізувавши роботи науковців в галузі кадрової безпеки, пропонуємо означити основними складовими кадрової безпеки зображено на малянку  2.

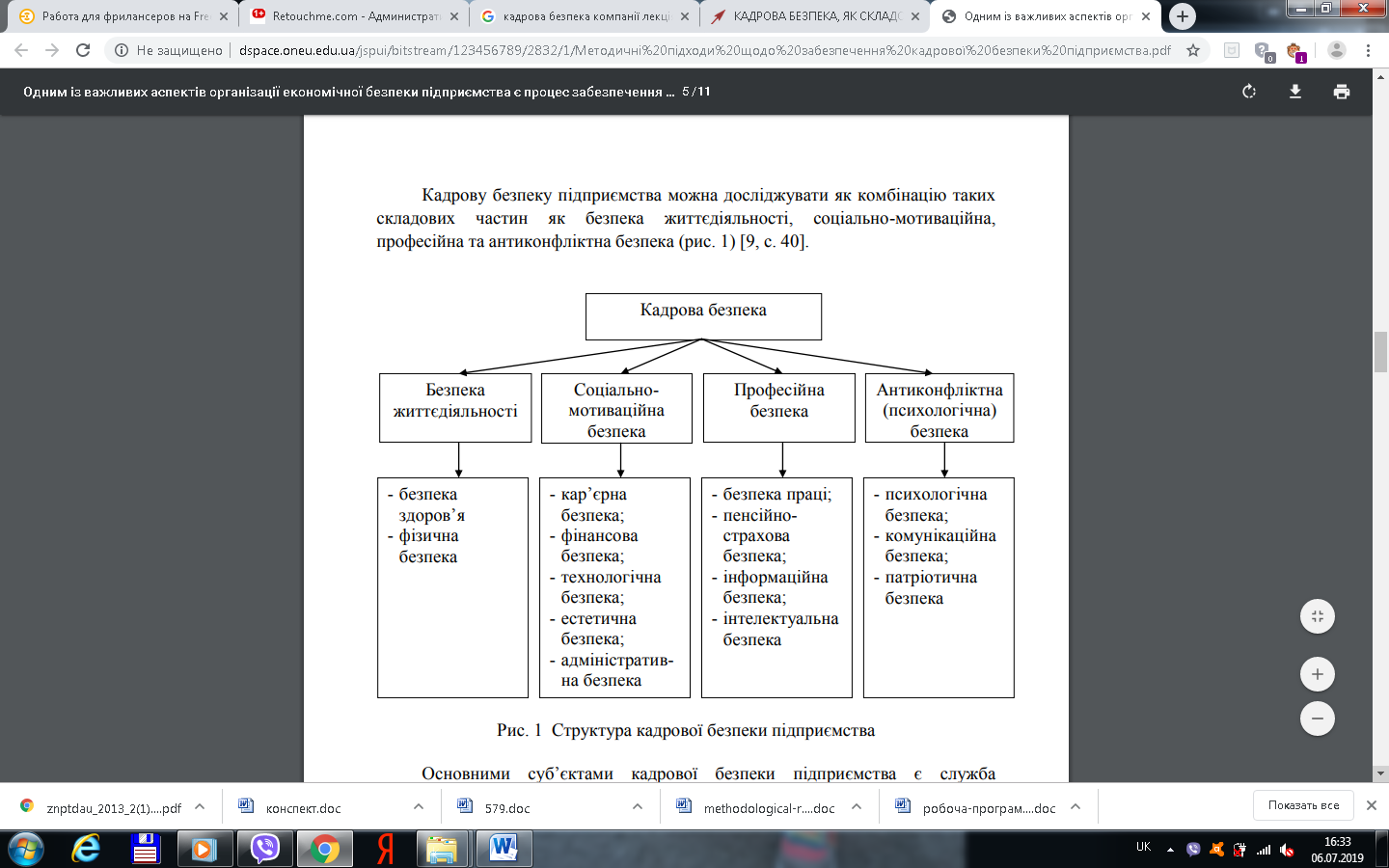


Рис. 2.  Складові кадрової безпеки

Проаналізувавши роботи науковців в галузі кадрової безпеки, пропонуємо системний підхід, а саме розглянути запропоновані основні складові кадрової безпеки банківської установи та ризик менеджмент, що мінімізує актуальні загрози кадровій безпеці та направлений на зниження ризиків конкретної складової кадрової безпеки.

Соціально-мотиваційна складова кадрової безпеки нараховує такі елементи:

■ кар'єрна безпека – професійно-кваліфікаційне та посадове просування працівників, заохочення в підвищенні своєї кваліфікації до вимог функціональних обов'язків, у гарантіях виробничого зростання, отримання шансів для самореалізації на робочому місці;

■ фінансова безпека – грошова забезпеченість, яка відповідає обсягу, кваліфікації, якості виконаної роботи; упевненість працівників у своєму робочому місці, стабільності оплати праці;

■ технологічна безпека – система аналізу та прогнозування, направлена на створення сучасного обладнання робочого місця, новітніх технологій, використання передового досвіду;

■ естетична безпека – проведення загальноосвітніх семінарів, конференцій, групових дискусій; мотивація задоволення персоналу своєю роботою; поліпшення власного іміджу кожного працівника;

■ адміністративна безпека – забезпечення об'єктивного оцінювання результатів праці та виявлення потенціалу кожного працівника, неможливість призначення непідготовлених і некомпетентних кадрів, що перебувають у родинних стосунках із власниками (засновниками, акціонерами тощо) підприємства, на керівні посади, на які заслужено претендують перспективні та досвідчені співробітники.

До складу професійної безпеки зараховують:

■ пенсійно-страхову безпеку – соціальний захист працівників, їх страхування, преференції якісного медичне обслуговування;

■ безпеку праці – створення безпечних умов праці на підприємстві;

■ інтелектуальну безпеку – рівень володіння сучасними знаннями, упровадження новацій у розвиток персоналу, підвищення рівня професійних знань, навичок, умінь, стимулювання прояву ініціативи та здібностей шляхом створення гнучкої системи преміювання відповідно до розвитку науково-технічного прогресу.

Найпоширенішими видами порушень з боку персоналу підприємства є такі:

■ фальсифікація сум готівки в касі та коштів на банківських рахунках, підробляння фінансових документів підприємства;

■ несанкціонований продаж і використання майна підприємства з корисливою метою;

■ оплата роботи підставних ("фіктивних") осіб;

■ фальсифікація документації підприємства за допомогою електронної техніки та Інтернету;

■ несанкціоновані операції з цінними паперами, матеріальними і нематеріальними активами підприємства;

■ повідомлення конфіденційної та іншої інформації третім особам;

■ фальсифікація звітів про використання коштів, виділених на відрядження, "представницькі видатки", на інші потреби підприємства.

Працівники підприємства можуть вдаватися до здійснення афер з різних мотивів, серед яких найпоширенішими є:

■ особисті фінансові труднощі, неможливість задоволення життєвих потреб;

■ низька кваліфікація керівництва підприємства;

■ нездоровий діловий клімат у колективі підприємства (наявність "скривджених");

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

■ порочні зв'язки, вчинки, захоплення;

■ слабкий кадровий менеджмент, неефективна персональна робота з кадрами.

**4.Управління кадровими ризиками.**

Вивченням і управлінням кадровими ризиками (кадрової безпекою) займається служба управління персоналом (служба управління людськими ресурсами, HR -менеджери), яка є суб'єктом кадрової безпеки. Її основна мета - виявлення, аналіз, запобігання і прогнозування потенційних загроз з боку співробітників організації, здатних порушити стійкість, розвиток і привести до зупинки її діяльності.

Найважливішим елементом кадрової безпеки слід вважати комплектування самої служби управління персоналом грамотними, висококваліфікованими фахівцями, які компетентні у вирішенні всього комплексу питань *HR* -менеджменту. В іншому випадку можливі ситуації ризику в результаті помилок в підборі персоналу, найм і звільнення, у плануванні, оцінці, розвитку, мотивації і стимулюванні персоналу.

З позиції служби управління персоналом кожен кандидат на вакансію в організації, так само як і кожен працівник підприємства, повинен постійно розглядатися як джерело кадрового ризику і потенційної загрози. В даний час до ризиків, що виникають в підсистемі управління персоналом організації, відносять наступні загрози з боку співробітників:

- Пряме розкрадання майна підприємства;

- Використання ресурсів підприємства у власних цілях;

- Навмисне псування і знищення майна підприємства;

- Отримання заробітної плати за невиконуючу роботу;

- Шантаж повноваженнями (це можливо, якщо вони зосереджуються в одних руках);

- Торгівля відомостями, що становлять комерційну таємницю;

- Порушення трудової дисципліни;

- Створення в колективі несприятливого моральнопсіхологіческого клімату.

При цьому під кадровою загрозою розуміється негативний вплив кадрової функціональної складової на економічну безпеку підприємства.

Виділяють два види загроз:

- Зовнішні, які не залежать від волі і свідомості працівників організації;

- Внутрішні, які визначаються діями (умисними чи ні) співробітників компанії.

Виділяють такі основні джерела загроз з зовнішнього середовища:

- Корумповані представники органів влади (проведення перевірок або оперативних заходів в ініціативному порядку або на замовлення конкурентів з метою закриття підприємства або вимагання хабарів);

- Підприємства-конкуренти, що здійснюють різного роду акції (у тому числі прямі погрози, шантаж, економічне шпигунство тощо);

- Кримінальні структури (прямий тиск на підприємство та його партнерів, організація нападів на підприємство і його власність тощо);

- Підприємства-постачальники (зміна цінової політики та зміну умов поставки ресурсів, сировини і комплектуючих);

- Підприємства-споживачі (відмова від закупівель продукції, вимоги про зміну цін та умов поставки і т.п.);

- Фахівці з інформаційних технологій, які не є співробітниками підприємства, несанкціоновано проникаючі в систему інформаційних ресурсів;

- Фінансово-кредитні установи (несподівана відмова в кредиті або затримка проводки платежів).

Джерелами внутрішніх загроз можуть бути співробітники компанії. При цьому можна виділити наступні три рівні:

- Перші керівники і топ-менеджери (пряме шахрайство, фальсифікація звітності, розкрадання майна, отримання відкатів, надання або продаж конкурентам інформації, що є комерційною таємницею підприємства);

- Менеджери, співробітники-фахівці основних і допоміжних виробництв (пряме злодіяння фінансових, інформаційних засобів та продукції, нецільове використання техніки, обладнання, інформаційно-обчислювальних засобів та ін., Продаж відомостей, що становлять комерційну таємницю підприємства, та ін.);

- Робітники (злодіяння готової продукції, сировини, комплектуючих, фінансових коштів, нецільове використання транспортних засобів і спеціальної техніки та обладнання, умисне виведення з ладу техніки, обладнання, інформаційних ресурсів, псування сировини та ін. за винагороду на замовлення третіх осіб та ін.).

При цьому мова йде не тільки про можливості умисного нанесення шкоди, а й, наприклад, про недовикористання трудового потенціалу. Сучасна наука і практика виділяють три основних якісних характеристики трудового потенціалу особистості. По-перше, психофізіологічний потенціал (стан здоров'я, тип вищої нервової діяльності, тип працездатності, особливості індивідуально-психологічних властивостей особистості і т.п.). По-друге, професійно-кваліфікаційний потенціал. І, нарешті, соціально-особистісний, що включає інтереси, мотиви, цінності і ціннісні орієнтації. Недовикористання трудового потенціалу може призвести до виникнення у працівників уявлень про неможливість застосування власного високого професіоналізму, неадекватності оцінки результатів праці, а отже, про невідповідність винагороди прикладеним трудовим зусиллям, викликати невдоволення змістом та умовами праці і т.д.

На виникнення внутрішніх загроз можуть вплинути наступні фактори: невисокий рівень розвитку системи управління персоналом; неграмотний підбір персоналу; недостатня кваліфікація персоналу; невірно вибудувана система мотивації; неефективна система навчання та розвитку персоналу; недостатня соціальна інформованість працівників про справи компанії, системи мотивації, просуванні персоналу і т.п .; нерозвинена організаційна культура; недооцінка значення лояльності персоналу.

Таблиця 4. Методи запобігання загрозам кадровій безпеці підприємства

|  |  |
| --- | --- |
| Загрози | Методи запобігання |
| Замах на фінансові та інші ресурси підприємства | Чітке ведення бухгалтерського та фінансового обліку діяльності, аудит документації, ретельна увага до добору персоналу та його стану, аналіз показників рентабельності та прибутковості діяльності підприємства |
| Дестабілізація організації, руйнування стабільного працездатного колективу (команди) | Ретельний добір персоналу, нагляд за відносинами в колективі, за комунікаціями на підприємстві, перевірка всіх підозрілих працівників на належність до будь-якої групи ризику, статистичний нагляд та аналіз руху персоналу |
| Погіршення дисципліни в колективі, порушення техніки безпеки та правил внутрішнього трудового розпорядку | Нагляд за відносинами в колективі, за комунікаціями на підприємстві, перевірка всіх підозрілих працівників на належність до будь-якої групи ризику, запобігання та розв'язання будь-яких конфліктів у колективі, чітка регламентація субординації і трудового розпорядку |
| Здійснення таємної протизаконної діяльності на підприємстві | Контроль за всіма комунікаціями на підприємстві, увага до взаємовідносин у колективі, аудит документації, вимога обов'язкової звітності про будь-які ділові операції в рамках підприємства |
| Сприяння утворенню конфліктів | Нагляд за відносинами в колективі, за діяльністю колективу й окремих працівників, чітка регламентація відносин, використання послуг медіаторів, сприяння згуртованості колективу, підвищення прихильності персоналу |

Сильна організаційна культура може частково, якщо не цілком, вирішити проблему управління ризиками. Це може здійснитися в тому випадку, якщо весь управлінський персонал буде зацікавлений не тільки в отриманні прибутку, а й в адекватному управлінні кадровими ризиками. Крім того, сильна організаційна культура передбачає наявність корпоративних стандартів поведінки, відображених, наприклад, у корпоративному етичному кодексі, де визначено необхідні для компанії моделі поведінки співробітників. Проведення роз'яснювальної роботи з персоналом із приводу норм, принципів організаційної культури та ефективної поведінки, встановлення з співробітниками довірчих відносин може сприяти запобіганню цілого ряду проблем, пов'язаних з кадровою безпекою.

Таким чином, якщо в організації виникають кадрові ризики, то це багато в чому означає, що служба управління персоналом не справляється зі своєю роботою, оскільки саме вона є суб'єктом кадрової безпеки, а будь-яка дія співробітників служби управління персоналом веде або до посилення, або до ослаблення безпеки організації.

**Висновок.**

1. На даному етапі кадрова безпека знаходиться в активному розвитку, а також є темою, яка цікавить більшість підприємців, які застосовують прогресивні, ефективні, науково обґрунтовані методи управління. Від кадрової безпеки залежить те, наскільки впевнений може бути керівник фірми в компетентності своїх працівників, в тім, що підприємство не піддасться небезпеці з вини персоналу.

2. Процес захисту підприємства від небезпеки починається на етапі підбору працівників на існуючі вакансії. А саме буквально з першої хвилини, коли особа, яка займається відбором персоналу, бачить кандидата на працевлаштування. І цей процес захисту існує безперервно у весь період функціонування підприємства, точно так, як безперервно функціонує на ньому його персонал.

3. Результативність у системі кадрової безпеки залежить від чіткої і ефективної взаємодії підрозділів. Відповідно до принципів розподілу повноважень і компетенції, в кожній компанії мають бути утворені горизонтальні зв'язки управління активами (часом, фінансами, людьми, інформацією) між кадровою службою та іншими службами і відділами.

4. Запропоновані методичні підходи націлені на таку роботу з персоналом, на встановлення таких трудових і етичних відносин, які сприятимуть розвитку і вдосконаленню управління кадровою безпекою підприємства.

**Завдання для самостійної роботи**

1. Причини послаблення кадрової безпеки на підприємстві. Необхідність забезпечення кадрової безпеки. Визначення причин через які "людський фактор" перетворюється на реальну загрозу кадровій безпеці організації. Причини ідеологічного, політичного, соціально-економічного, психологічного, морального, національного, природного та техногенного характеру.

2. Класифікація ризиків та загроз кадровій безпеці. Наведення класифікації ризиків та загроз кадровій безпеці. Небезпеки і загрози безпеці підприємства залежно від джерела виникнення, від можливості запобігання та залежно від об'єкта замаху. Визначення загроз за характером втрат від їх реалізації, за економічним характером, за джерелом (суб'єктом) загрози.

3. Дослідження методів попередження загроз кадровій безпеці підприємства. Класифікація методів протидії загрозам кадровій безпеці за часом реалізації, за характером дії і за ступенем легітимності.

**Питання для самоконтролю**

1. Дайте визначення поняттю кадрова безпека

2. Назвіть основні складові кадрової безпеки

3. Методи запобігання загрозам кадровій безпеці підприємства

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Проблеми управління економічною безпекою суб'єктів господарювання: Монографія /О. А. Кириченко, В. С. Сідак та ін. – К.: Університет «КРОК», 2008. – 403 с.

2. Лащенко О. Ю. Кадрова безпека як підсистема в системі економічної безпеки підприємства [Електронний ресурс] / О. Ю.Лащенко. — Режим доступу: http://www.nbuv.gov. ua/e-journals/pspe/2007-3/laschenko\_307.htm.]

3. Н. Г.Мехеда, А. І.Маренич соціально-мотиваційні складові кадрової безпеки (с.46) Financial Space № 2 (6) 2012)

4. Кибанов А. Я. Управление персоналом организации. – М.: ИНФРА-М, 2002. – 638 с.

5. Чумарин И. Работа с персоналом в контексте общей безопасности компании / И. Чумарин // Менеджмент по персоналу. — 2005. — № 1. — С. 34–40.

6. Логінова Н. І. Місце кадрової безпеки в економічній безпеціпідприємства / Н. І. Логовіна //Коммунальное хозяйство городов : Научно-технический сборник. - 2009. - № 87. - С. 371-376.

7. Васильчак С. В. Кадрова безпека підприємства — основа економічного розвитку / С. В. Васильчак, І. Р. Мацюняк // Науковий вісник НЛТУ України. — 2009. — № 7. — с.23–26.

8. О. М. Герасименко, Моделювання системи забезпечення кадрової безпеки суб'єкта господарювання, Економііка та управлііння піідприємствами - актуальні проблеми економіки №2(128), 2012 с.118 -124, с. 119.

9. Козаченко А. В., Пономарев В. П., Ляшенко О. М. Экономическая безопасность предприятия: сущность и механизмы обеспечения: Монография. – К.: Либра, 2003. – 280 с.

**Лекція №11**

**Тема. Організація взаємодії орану безпеки компанії з правоохоронними та контролюючими органами**

**Мета:** пошук оптимального поєднання взаємодії органів безпеки компанї з правоохороними та контролююими органами

**План**

1. Організація взаємодії з правоохоронними органами щодо гарантування безпеки бізнесу

2. Організація взаємодії структурних підрозділів, установ, організацій, підприємств для проведення спільних заходів із протидії ризикам і загрозам

3. Стратегія забезпечення економічної безпеки підприємства, установи, організації

**Вступ**

Головною діючою особою ринку в недержавному секторі економіки і стрижнем будь-якої економічної системи, побудованої не на державномонополістичних, а на конкурентних засадах є підприємець. Підприємець виступає гарантом стабільності цивільного суспільства, гарантом економічної безпеки держави. Але необхідно зазначити, що повсякденна практика недержавних об'єктів економіки свідчить про їх підвищену порівняно з державними структурами уразливість від протиправних та інших посягань з боку різного роду кримінальних структур, а також окремих осіб. Власність тепер зобов'язує підприємців займатись діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є підґрунтям функціонування недержавних об'єктів. Отже, охорона підприємництва і забезпечення безпеки підприємницької діяльності є стрижневою проблемою, що обіймає комплекс організаційно-правових, техніко-технологічних, адміністративних, виховних, фінансових і спеціальних заходів, спрямованих на виявлення, попередження і припинення загроз і зазіхань на стабільність функціонування і розвитку підприємства. Цей процес містить у собі охорону приватної власності підприємства і фізичний захист його персоналу. При цьому до власності відносять, по-перше, основне матеріальне майно: приміщення, земельна ділянка, парк техніки, сировина й інвентар, а також допоміжне устаткування, призначене для збереження, переробки і перевезення вантажів. По-друге, сюди ж варто віднести інтелектуальну власність, що складає інформацію, яка є активом компанії про власність власника, а також знання і досвід співробітників підприємства, їхні професійні секрети і винаходи. Підприємці, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення, як необгрунтовано високі, оскільки життя цінується набагато вище. Нещастям вітчизняних підприємців є те, що, заробивши великі гроші, вони не хочуть усвідомлювати, що багатство неминуче переводить їх у "групу ризику". Як показує сумний досвід, наші підприємці починають здійснювати суттєві кроки із забезпечення власної безпеки лише після того, як у них починаються неприємності.

**1. Організація взаємодії з правоохоронними органами щодо гарантування безпеки бізнесу**

Взаємодія. Для забезпечення безпеки підприємства необхідно, щоб зусилля всіх осіб, що її забезпечують, підрозділів, служб були скоординованими. Всі учасники даного процесу повинні взаємодіяти один з одним. Вони повинні чітко знати, хто за що несе відповідальність і яку роботу виконує. Від узгодженості діяльності всіх учасників процесу залежить успіх справи, кінцевий результат та досягнення поставленої мети.

Принцип взаємодії передбачає також встановлення тісних ділових зв'язків та узгодження дій із зовнішніми організаціями (правоохоронними органами, місцевими та районними службами безпеки, органами влади тощо), що здатні надати необхідну допомогу в забезпеченні безпеки підприємства.

Поєднання гласності та конфіденційності. Система основних заходів безпеки повинна бути відома всім співробітникам підприємства, з метою забезпечення безпеки її вимоги повинні виконуватись. Це дозволить вчасно виявити потенційні і реальні небезпеки та загрози та запобігти їм. Одночасно цілий ряд способів, сил, засобів, методів забезпечення безпеки повинні бути засекречені та відомі лише вузькому колу осіб. Це дає можливість більш ефективно боротися як з внутрішніми, так і з зовнішніми загрозами, вчасно запобігати нанесенню шкоди підприємству.

Компетентність. Питання забезпечення безпеки підприємства є не другорядним, а життєво необхідним. В результаті дій зловмисників, не­добросовісної конкуренції, прийняття дуже ризикованих рішень тощо підприємству може бути нанесено непоправної шкоди, тому питаннями забезпечення безпеки підприємства повинні займатись професіонали, що знають суть проблеми, вміють вчасно оцінити ситуацію та прийняти правильне рішення.

Система безпеки підприємства будується у відповідності до політики, що проводиться, та стратегії безпеки.

Політика безпеки підприємства [3] являє собою систему поглядів, заходів, рішень, дій в галузі безпеки, що створюють умови, сприятливе середовище для досягнення цілей бізнесу.

Тобто, політика безпеки, що проводиться, дозволяє підприємству виконувати виробничу програму, виробляти конкурентоспроможну продукцію (товари, роботи, послуги), підвищувати ефективність виробництва, примножувати власність, отримувати необхідний прибуток тощо.

Під стратегією безпеки [1] розуміють сукупність найбільш важливих рішень, направлених на забезпечення програмного рівня безпеки функціонування підприємства.

Стратегії безпеки за своїм змістом бувають різноманітними. Можна виокремити три типи.

Стратегія, пов'язана з необхідністю раптового реагування на загрози (виробничій діяльності, майну, персоналу тощо), що виникають. Тобто в даному випадку діє принцип "загроза — відбиття". Створені (найчастіше поспішно) для вирішення цього завдання підрозділи, служби, виділені сили та засоби можуть послабити або запобігти дії загрози, але може виникнути ситуація, коли підприємству буде завдана шкода.

Стратегія, орієнтована на прогнозування, завчасне виявлення небезпек та загроз, цілеспрямоване дослідження економічної та криміногенної ситуації як всередині підприємства, так і в оточуючому його середовищі. Виділені для рішення такого завдання спеціалісти, сформовані підрозділи та служби безпеки створюють можливість свідомо і цілеспрямовано проводити роботу з формування сприятливих умов для підприємницької діяльності.

Стратегія безпеки, направлена на відшкодування (відновлення, компенсацію) нанесених збитків. Така стратегія може вважатись доцільною лише тоді, коли збитки можна відшкодувати, або коли немає можливості здійснити стратегію першого та другого типів.

У розумінні "системи безпеки підприємства" не існує єдиної думки [6]. Наприклад, на погляд В. П.Мак-Мака, система безпеки підприємства включає наукову теорію безпеки, політику та стратегію безпеки, засоби та методи забезпечення безпеки і концепцію безпеки підприємства [6].

В. І. Ярочкін визначає систему безпеки як організовану сукупність спеціальних органів, служб, засобів, методів та заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства, держави від внутрішніх та зовнішніх загроз [5, с.9].

Надумку О. А. Груніна та С. О. Груніна система безпеки підприємства являє собою обмежену множину взаємопов'язаних елементів, що забезпечують безпеку підприємства та досягнення ним цілей бізнесу.

З початком ринкових реформ паралельно з державними почали виникати різноманітні приватні охоронні та детективні організації, аналітичні центри, інформаційні служби; навчальні, наукові та консультаційні організації тощо. Вони, як правило, за оплату надають послуги щодо охорони об'єктів, забезпечують захист інформації, комерційної таємниці, накопичують та надають інформацію щодо конкурентів, ненадійних партнерів і т. ін. Світовий досвід свідчить, що в основному саме недержавні організації вирішують завдання щодо забезпечення безпеки підприємництва.

Формування системи безпеки та передусім створення її органів (суб'єктів) залежить від розмірів підприємства, його економічних, фінансових, виробничо-технічних, інформаційних, інтелектуальних, професіональних, організаційних та інших можливостей.

Як свідчить досвід малі підприємства найчастіше користуються послугами зовнішніх спеціалізованих приватних організацій: консалтингових, охоронних, інформаційних. До них відносяться реєстраційні палати, фірми, що займаються підбором та атестацією кадрів, кредитні бюро, які надають інформаційні послуги щодо ділового реноме партнерів, їх платоспроможності, центри маркетингових досліджень, приватні охоронні й детективні організації та ін.

Середні підприємства можуть використовувати комбіновану систему безпеки: з одного боку, у випадку необхідності отримувати послуги від зовнішніх організацій, з іншого — активно спиратися на можливості власних служб та підрозділів. Наприклад таких, як юридичний та фінансовий відділи, та служб маркетингу, охорони, техніки безпеки, кадрів, економічного аналізу, пропускного режиму, діловодства. З метою підвищення ефективності діяльності служб та підрозділів, які займаються захистом економічних інтересів фірми, на підприємстві повинен бути створений координуючий орган або призначений один з керівників відповідальним за економічну безпеку.

Для великого підприємства доцільним буде створення власної служби безпеки. Як правило, всю діяльність щодо забезпечення безпеки координує один з керівників підприємства. Для вироблення пропозицій та виконання консультативних функцій може створюватись рада з безпеки. Служба безпеки може включати найрізноманітніші відділи, групи, підрозділи. До найбільш значущих слід віднести підрозділи: охорони, режиму, роботи з кадрами, спеціального документообороту з грифом "КТ", інженерно-технічного захисту, розвідки та контррозвідки, інформаційно - аналітичної діяльності, оперативного реагування, кризову групу.

Одним з найбільш значимих елементів системи безпеки підприємства є механізм її забезпечення, який являє собою сукупність законодавчих актів, правових норм, рушійних мотивів та стимулів, методів, заходів, сил та засобів, за допомогою яких суб'єкт впливає на об'єкт для досягнення цілей безпеки та вирішення завдань.

Сили та засоби, що використовуються, як правило, розподіляються на декілька груп : фінансові, кадрові, організаційні, технічні, інформаційні, правові, інтелектуальні тощо. За допомогою них вирішуються завдання щодо забезпечення безпеки. Так, наприклад, за допомогою технічних засобів, таких як відео-, радіоапаратура, охоронно-пожежні системи тощо вирішують завдання щодо спостереження за об'єктами. За допомогою організаційних заходів створюють спеціальні підрозділи, зони безпеки, спеціальні пости, патрулі і т. ін. Фінансові засоби необхідні для придбання технічних пристроїв безпеки, утримання служби безпеки, підготовки кадрів, стимулювання праці. Аналогічним чином за призначенням використовуються й інші сили та засоби.

Система безпеки підприємства вирішить завдання, що перед нею поставлені, тоді, коли буде працювати, тобто її невід'ємною складовою є практичні дії щодо забезпечення безпеки бізнесу.

Таким чином, в результаті вивчення сутності економічної безпеки підприємства можна зробити висновок, що вона покликана створити умови для ефективної діяльності підприємства та, в результаті, досягнення цілей бізнесу в умовах конкуренції та господарського ризику, шляхом своєчасного виявлення та послаблення дії різноманітних небезпек та загроз.

Якою б узгодженою не була самоорганізація безпеки підприємницької організації, вона не забезпечить запобігання злочинним посяганням без взаємодії з відповідними правоохоронними органами і насамперед з поліцією.

Організаційно-правовою основою такої взаємодії е:

- конституційні принципи рівності захисту всіх форм власності;

- закони України про Національну поліцію, про оперативно-розшукову діяльність, про прокуратуру та інші нормативно-правові акти;

- угода між МВС України і асоціаціями та громадськими об'єднаннями підприємців, споживачів, охоронних підприємств і детективних агентств про взаємодію в галузі гарантування безпеки і боротьби зі злочинністю.

Метою співпраці є запобігання злочинним посяганням на персонал комерційних підприємств та розкриття їх цінності.

Пріоритетними напрямами взаємодії підприємства і структурними підрозділами Національної поліції мають бути:

Обмін інформацією:

- про факти (способи) розкрадань грошових коштів з використанням підроблених банківських документів, кредитних карток, інших документів;

- про фізичних осіб, що працюють у комерційних підприємствах, підозрюваних у скоєнні злочинів.

Розроблення сумісних заходів:

- протидії передбачуваним (реальним) кримінальним проявам, загрозам убивства або тяжких тілесних ушкоджень, знищенню майна підприємств, їх керівників, співробітників та членів їх сімей;

- із технічної оснащеності засобами сигналізації об'єктів;

- зі створення так званої "гарячої лінії" між службами безпеки і територіальними органами поліції;

- участь у формуванні централізованого, регіонального підприємства даних про підприємства різних форм власності, недобросовісних учасників ділових операцій, кримінальних авторитетів та ін.

Робота з підбору, розстановки, професійної, спеціальної підготовки персоналу служби безпеки:

- здійснення сумісної перевірки кандидатур на роботу в службу безпеки з використанням інформаційних можливостей органів Національної поліції, відомостей про судимість та ін.;

- сумісне розроблення і введення правил про відповідальність персоналу за протиправне використання або розголошування комерційної таємниці;

- використання допомоги поліції в навчанні і підвищенні кваліфікації кадрів служби безпеки.

Здійснення поліцією оперативно-розшукової роботи щодо поданих службою безпеки неспростовних матеріалів про злочинні дії працівника, що сховався, або іншої особи. Служби безпеки фірм, компаній, організацій координують свою діяльність і взаємодіють між собою на основі укладеного договору. Координація і взаємодія між ними полягають в:

- обміні оперативною інформацією;

- сумісному аналізі;

- сумісному плануванні з окремих питань і напрямів діяльності;

- взаємному використанні наявних сил і засобів;

- сумісному проведенні відкритих і закритих заходів оперативного характеру.

Взаємодія служб безпеки фірми, компанії з державними правоохоронними органами є дуже серйозною і значною мірою ще не до кінця законодавчо розв'язаною проблемою. Тому досі в діяльності цих органів і підприємницьких компаній існує чимало проблем і навіть суперечностей. Це нерідко призводить до незахищеності підприємців перед неправомірними діями працівників поліції та контрольних органів і навіть до порушення їх прав і свобод як громадян і власників.

Багато підприємців мають негативний досвід спілкування з працівниками поліції. Зневага правами громадянина, образи, рукоприкладство, необґрунтовані звинувачення, на жаль, не такі вже й рідкісні в практиці правоохоронних органів. Причин тому кілька. Головні-це традиції, що історично склалися, низька правова культура суспільства в цілому. Зловживання працівників правоохоронних органів

**2. Організація взаємодії структурних підрозділів установ, організацій, підприємств для проведення спільних заходів із протидії ризикам і загрозам**

Концепція є методологічною основою побудови системи економічної безпеки фірми та її підрозділів і призначена для використання при плануванні та здійснені відповідних заходів, виходячи з вимог Конституції України, Закону України „Про основи національної безпеки України”, інших законів, що регламентують діяльність атомноенергетичної галузі, указів Президента України, нормативно-правових актів Уряду та відповідних внутрішніх документів фірми.

Основними цілями забезпечення економічної безпеки є участь підрозділів економічної безпеки разом з іншими підрозділами в досягненні максимальної стабільності функціонування установи та створення найбільш сприятливих умов для її подальшого розвитку шляхом попередження можливих загроз та негативних впливів на фінансовоекономічну діяльність фірми.

Організація заходів пов’язаних з економічною безпекою установи базується на наступних основних принципах:

- безумовне виконання норм діючого законодавства України та інших нормативно-правових актів, які регулюють питання організації економічної безпеки;

- організація та функціонування ефективної системи підрозділів економічної безпеки для попередження негативних фінансово-економічних наслідків для установи;

- вибору і співпраці з діловими партнерами на засадах конкурентного середовища та прозорості прийняття рішень. Надання пріоритетів якості та надійності у постачанні товарів, робіт та послуг за умови економічної обґрунтованості їх вартості;

- вдосконаленні і розвитку внутрішньої системи підрозділів економічної безпеки, захисті конфіденційної комерційної інформації установи та її контрагентів, забезпеченні разом з персоналом інших підрозділів економного та раціонального використання економічних та фінансових ресурсів, збереження власності фірми;

- вжиття необхідних заходів по попередженню та недопущенню персоналом установи випадків завдання економічних та фінансових збитків з корисних мотивів або недбалого виконання своїх професійних обов’язків.

Зазначені принципи реалізуються комплексно, безперервно, оперативно та централізовано, зокрема:

• Комплексність передбачає системність вирішення питань економічної безпеки, із задіяням усіх суб’єктів, активів та інтересів установи.

• Безперервність – це постійний системний моніторинг підрозділами економічної безпеки даних про фінансово-економічний стан контрагентів та його аналіз з метою недопущення, як внутрішніх, так і зовнішніх загроз діяльності устаеови.

• Оперативність – це швидкість реагування на виникнення ризиків та загроз, своєчасність доповіді Керівництву для прийняття попереджувальних управлінських рішень.

• Централізація – це єдиний підхід підрозділів економічної безпеки установи до виконання своїх функцій при координуючій ролі та методичному керівництві з боку підрозділу економічної безпеки Дирекції установи.

Нагадаємо, що під загрозами розуміють чинники, що негативно впливають на стан однієї чи кількох функціональних складових економічної безпеки установи. Слід відрізняти внутрішні і зовнішні загрози.

Зовнішні загрози – це дії, явища або процеси, що не залежать від волі та свідомості працівників установ.

Внутрішні загрози – це дії (навмисні або необережні) працівників установ та їх підрозділів, що можуть потенційно нанести збиток установ. Суб’єктами економічної безпеки установ вважається усі особи та організації, які приймають участь у забезпеченні економічної безпеки установ. Суб’єктами економічної безпеки розподіляються на внутрішні та зовнішні.

Внутрішніми суб’єктами забезпечення економічної безпеки є:

• Дирекція установ;

• підрозділ економічної безпеки установ;

• підрозділи економічної безпеки відокремлених підрозділів (далі ВП);

• підрозділи Дирекції та ВП установ;

• окремі посадові особи, які наділені відповідними повноваженнями згідно внутрішніх нормативних актів;

• весь персонал установ.

Зовнішніми суб’єктами забезпечення економічної безпеки установ можуть бути:

• представники правоохоронних органів;

• підрозділи економічної безпеки контрагентів, що співпрацюють з установою

• інші суб’єкти (в т.ч. іноземні), які співпрацюють з установою, де є відповідні підрозділи.

Основні засади розподілу компетенції суб’єктів у сфері забезпечення економічної безпеки установ.

Компетенція Дирекції установ:

• розробка політики забезпечення економічної безпеки;

• безпосереднє керівництво підрозділами економічної безпеки Дирекції та відокремлених підрозділів (ВП);

• визначення інтересів та пріоритетів у сфері економічної безпеки;

• підготовка, розгляд та затвердження документів, що регламентують основні питання взаємодії підрозділів фірми у сфері економічної безпеки. Компетенція підрозділу економічної безпеки Дирекції установ:

• розробка, затвердження та контроль за виконанням нормативно-правових актів, які забезпечують економічну безпеку у підрозділах фірми;

• виконання інших завдань, що покладені Керівництвом установи у сфері забезпечення економічної безпеки;

• взаємодія із правоохоронними органами та підрозділами економічної безпеки (де вони є, або підрозділами загальної безпеки) з питань, що входять до компетенції підрозділів економічної безпеки фірми;

• координація діяльності підрозділів економічної безпеки ВП, надання їм методичної допомоги, вивчення та розповсюдження позитивного досвіду роботи;

• проведення зовнішніх та внутрішніх заходів з одержання інформації, згідно компетенції підрозділу, а також ведення інформаційно-аналітичної роботи;

• аналіз ризиків для діяльності установ та своєчасне доведення отриманої інформації Керівництву установи для прийняття відповідних управлінських рішень;

• проведення заходів щодо протидії негативним впливам на фінансово економічну діяльність установи, взаємодія із зазначених питань із правоохоронними та спеціальними службами, а також органами влади та управління, іншими зовнішніми суб’єктами у сфері економічної безпеки. Діяльність підрозділів економічної безпеки відокремлених підрозділів установ координується, методично і методологічно забезпечується підрозділом економічної безпеки Дирекції фірми.

До завдань та функцій зазначених підрозділів, крім визначених для підрозділу економічної безпеки Дирекції Керівництвом ВП можуть бути надані додаткові функції, що не суперечать їх компетенції, але тільки після узгодження з підрозділом економічної безпеки Дирекції та затвердженням Керівництвом установи. Компетенція інших підрозділів установи з питань економічної безпеки:

• порушення проблемних питань з економічної безпеки перед Керівництвом установи та підрозділами економічної безпеки;

• виконання управлінських та розпорядчих документів з питань економічної безпеки;

• участь у розробці та реалізації заходів із забезпечення економічної безпеки;

• негайне повідомлення Керівництва установи та підрозділу економічної безпеки про можливе відхилення від встановлених стандартів економічної безпеки;

• надання згідно порядку встановленому внутрішніми нормативними документами, відповідної інформації у підрозділи економічної безпеки;

• погодження із підрозділами економічної безпеки заходів, реалізація яких пов’язана з можливими фінансово-економічними ризиками для отримання відповідних висновків щодо конкретних контрагентів.

Компетенція персоналу установ з питань економічної безпеки:

• чітке виконання керівних документів та вказівок Керівництва Компанії з питань економічної безпеки;

• прогнозування можливих фінансово-економічних ризиків та збитків при плануванні своєї роботи та роботи підрозділів Дирекції та ВП;

• підтримання встановленого в установі режиму економічної безпеки;

• надання (відкрите чи анонімне) у підрозділи економічної безпеки інформації про можливі порушення в сфері економічної безпеки, проведення протиправних дій проти установи та її працівників, або самими працівниками і зовнішніми суб’єктами;

• надання всебічного сприяння підрозділам економічної безпеки у протидії загрозам, що можуть нанести збитки установи;

• передача до підрозділів економічної безпеки пропозицій з поліпшення системи забезпечення економічної безпеки установи;

• виконання встановлених вимог збереження та нерозголошення конфіденційної службової та комерційної інформації як установи, так і контрагентів.

Дана Концепція є основою для розробки Типових положень про підрозділи економічної безпеки установи, про організацію перевірки контрагентів, посадових інструкцій для працівників підрозділів економічної безпеки, наказів, розпоряджень, інших документів з питань забезпечення економічної безпеки. Відповідальність структурних підрозділів при проведенні заходів із забезпечення безпеки.

Обов’язки структурного підрозділу: Забезпечує організацію управління фінансово-економічним, майновим та інформаційним напрямами роботи підрозділу (відділу, сектору, групи). Організовує та координує напрямки робіт з розроблення, запровадження та реалізації заходів із забезпечення фінансово-економічної та інформаційної безпеки. Забезпечує дотримання підрозділом (відділом, сектором, групою) усіх зобов’язань із фінансово-економічної секретності. Забезпечує виконання підрозділом (відділом, сектором, групою) програм, планів щодо впровадження новітніх технологій у сфері фінансово-економічної та інформаційної безпеки, оновлення відповідних програмних забезпечень. Вживає заходів щодо забезпечення підрозділу (відділу, сектору, групи) працівниками з питань фінансов-оекономічної та інформаційної безпеки, найкращого використання їх знань і досвіду.

Під час виявлення зовнішніх і внутрішніх загроз і ризиків у сфері фінансово-економічної безпеки підрозділу (відділу, сектору, групи) спрямовує роботу на виконання відповідних процедур щодо їх усунення та зменшення. Вирішує питання щодо фінансово-економічної та інформаційної безпеки в межах наданих йому повноважень, доручає виконання окремих функцій підлеглим працівникам. Розроблює правовий статус структури підрозділів фінансово-економічної та інформаційної безпеки. Керує роботами зі створення та впровадження нових технологій щодо зниження загроз і ризиків діяльності підрозділу (відділу, сектору, групи), забезпечення фінансово-економічної та інформаційної безпеки. У межах наданих йому повноважень надає всім категоріям посадових осіб інформацію, яка стосується діяльності із забезпечення фінансово-економічної та інформаційної безпеки.

Контролює забезпечення підвищення кваліфікації працівників підрозділу (відділу, сектору, групи) у сфері фінансово-економічної та інформаційної безпеки. Сприяє захисту фінансово-економічних та інформаційних інтересів підрозділу (відділу, сектору, групи) в суді, органах державної влади й управління, приватних і юридичних осіб.

Забезпечує дотримання законності, активне використання правових засобів удосконалення управління та функціонування в ринкових умовах, зміцнення договірної, економічної та фінансової дисципліни.

**3. Стратегія забезпечення економічної безпеки підприємства, установи, організації**

Стратегія економічної безпеки – це економічна система забезпечення економічної безпеки у довгостроковому періоді, що являє собою сукупність індивідуальних для кожного суб’єкта господарювання взаємоузгоджених і взаємозумовлених складових, які об’єднує єдина глобальна мета – досягнення високого рівня прибутку. Ефективна стратегія економічної безпеки повинна включати: характеристику зовнішніх та внутрішніх загроз економічній безпеці суб’єкта господарювання; визначення та моніторинг факторів, що зміцнюють чи руйнують сталість його соціальноекономічного стану на короткострокову і середньострокову (три — п’ять років) перспективу; визначення критеріїв та параметрів (граничних значень) показників, що характеризують інтереси суб’єкта та відповідають вимогам його економічної безпеки; розробку економічної політики, що включатиме механізми обліку факторів, які мають вплив на стан економічної безпеки; напрями діяльності суб’єкта господарювання для реалізації стратегії.

У економічній літературі виділяють три типи стратегій забезпечення економічної безпеки суб’єкта господарювання. Проте можна виділити чотири типи стратегій економічної безпеки, що є прийнятними для застосування у компаніях з управління активами. Стратегія «передбачення». Прийняття до реалізації такої стратегії має на меті створення спеціального підрозділу або служби економічної безпеки у, завданнями якої стане:

• оцінка стану і динаміки розвитку;

• виявлення факторів (прямих та непрямих, внутрішніх та зовнішніх небезпек та загроз), що заважають розвитку та можуть мати вплив на її економічну стабільність;

• визначення причин, джерел, характеру та інтенсивності впливу загроз на потенціал;

• прогнозування наслідків впливу виявлених загроз на результативність роботи (розрахунок можливих збитків);

• розробка заходів щодо запобігання руйнівному впливу небезпек та загроз на стійкість та стабільність стану;

• розрахунок обсягів фінансування запропонованих заходів та співставлення отриманих даних з розмірами можливих збитків (за необхідності корегування розроблених заходів відповідно до виділеного бюджету фінансування діяльності механізмів економічної безпеки);

• проведення розроблених заходів та оцінка їх ефективності;

• виявлення відхилень показників ефективності реалізації заходів економічної безпеки зі встановленими нормативами.

Таким чином, дана стратегія включає проведення значної попередньої підготовки – аналізу, планування, прогнозування, виявлення загроз – заходів гарантування економічної безпеки компанії. Вона є найбільш витратною, і не може реалізовуватися при обмежених фінансових ресурсах. Проте така стратегія здатна забезпечити економічну незалежність компанії, стабільність і сталість її поточного фінансово-господарського стану та здатність до розвитку та майбутнього прогресу.

Стратегія «активного захисту». Фірма, що обирає дану стратегію, не створює службу економічної безпеки в якості нового структурного підрозділу. Аналіз небезпек і загроз та планування конкретних дій, щодо їх усунення або уникнення, не проводиться. За умови настання небажаних для компанії ситуацій, що матимуть негативні наслідки для її діяльності, менеджмент створює так звану «групу реагування» або заключає договір зі сторонньою фірмою чи організацією, яка надає послуги забезпечення економічної безпеки для різного виду суб’єктів господарювання. Наслідком обрання такої стратегії є негайне реагування на загрози, їх нейтралізація, оцінка рівня негативного впливу, запровадження заходів щодо його мінімізації, компенсування збитків та виявлення винних (якщо збитки були спричинені внутрішньою загрозою). Розміри необхідного фінансування такої стратегії не можуть бути визначені заздалегідь, оскільки залежать від конкретного виду небезпек та рівня їх впливу на компанію. Позитивною особливістю даного виду стратегії є те, що за відносної відсутності загроз для діяльності, компанія не витрачає значні суми коштів на планування заходів захисту, що можуть і не знадобитися, а інвестує їх у свій розвиток для отримання прибутку та підвищення рівня конкурентоспроможності.

Стратегія «пасивного захисту» (мінімізації збитків). Як і стратегія активного захисту, не передбачає процедур постійного моніторингу загроз та розробку заходів їх нівелювання. Мета даної стратегії зводиться до виявлення загрози, що уже розпочала свій негативний вплив на діяльність компанії та вжиття заходів щодо мінімізації та покриття збитків, що стали її наслідком. Основним способом реалізації стратегії може стати страхування майна та персоналу, а також персональної відповідальності окремих посадових осіб. Така стратегія економічної безпеки зводиться до розуміння можливості виникнення загрози діяльності компанії, але жодних дій щодо її упередження або уникнення не проводиться, проте після зникнення небезпеки або припинення її впливу на діяльність, проводяться заходи щодо недопущення повторного виникнення подібного виду ризиків. Стратегія «компенсації збитків». Відрізняється від попередньої стратегії лише тим, що при активному розгортанні кризових явищ у компанії, падінні її фінансових показників та втрати стабільності діяльності, не робиться ніяких спроб послабити причину виникнення негативних явищ або хоча б мінімізувати збитки, завдані компанії. Використання цього виду стратегії передбачає виділення певної суми коштів, у вигляді створення спеціального фонду або запланованих витрат на цільові заходи, які у випадку порушення нормального функціонування компанії компенсують завдані їй збитки (якщо, звісно, депонованих сум для цього вистачає). Використання двох останніх видів стратегій пропонується лише тим компаніям, що не мають фінансової спроможності застосувати стратегії перших двох типів, які дійсно здатні гарантувати економічну безпеку компаній з управління активами, а не лише фінансувати покриття збитків від відсутності чіткого механізму її забезпечення. Обрання стратегії формування економічної безпеки є важливим моментом в організації системи захисту діяльності та гарантування належного рівня її фінансової стабільності та рентабельності.

**Висновок.**

Закон України «Про охоронну діяльність» містить цілий ряд суперечливих положень, що стосуються понятійного апарату, переліку суб’єктів охоронної діяльності, взаємодії суб’єктів недержавної охорони та правоохоронних органів. Понятійний апарат слід удосконалити, перелік суб’єктів охоронної діяльності – розширити, перелік послуг – деталізувати. Законодавство щодо охоронної діяльності потребує підзаконного акту, який би врегулював формальні аспекти взаємодії між правоохоронними органами та приватними охоронними організаціями, що спрямована на попередження, припинення і розкриття кримінальних правопорушень та забезпечення охорони громадського порядку.

**Завдання для самостійної роботи**

1. Інформаційно-аналітична діяльність служби безпеки в зовнішньоекономічній сфері.

2. Вивчення клієнтів, конкурентів, ділових партнерів.

3. Протидія іноземній промисловій і технічній розвідці.

4. Забезпечення безпеки ділових переговорів.

5. Координація і взаємодія з державними спеціальними органами.

**Питання для самоконтролю**

1. Для забезпечення безпеки підприємства необхідно

2. Організація заходів пов’язаних з економічною безпекою установи

3. Компоненти стратегії економічної безпеки

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури.**

1. Новікова Н. І. Правова регламентація діяльності служби безпеки. Підприємства як складова його економічної безпеки / Н. І. Новікова // Ученые записки Таврического национального университета им. В. И. Вернадского. Серия «Юридические науки». – Т. 26 (65). – 2013 – № 2–1. – Ч. 1. – С. 352–357.

2. Про охоронну діяльність: Закон України від 22.03.2012 // Відомості Верховної Ради України. – 2013. – № 2. – Ст. 40.

3. Про затвердження переліку спеціальних засобів, придбання, зберігання та використання яких здійснюється суб’єктами охоронної діяльності : Постанова Кабінету Міністрів України від 11.02.2013 // Урядовий кур’єр. – 2017. – №4

**Лекція №12**

**Тема. Інформаційно-аналітична робота в корпоративній безпеці.**

**Мета:** визначення суті та ролі інформаційно-аналітичної діяльності у формуванні ефективної системи економічної безпеки суб'єктів підприємництва.

**План**

1. Зміст інформаційно-аналітичної діяльності: загальні поняття та визначення.

2. Організація інформаційно-аналітичної роботи в системі фінансово-економічної безпеки суб’єктів господарювання.

3. Суть інформаційно-аналітичної діяльності та її роль у формуванні ефективної системи економічної безпеки субєктів підприємництва.

**Вступ**

Система економічної безпеки вибудовується з урахуванням перерахованих завдань, умов конкурентної боротьби, специфіки бізнесу, технологічних особливостей, конкурентної стратегії, стадії життєвого циклу підприємства. Система економічної безпеки кожного підприємства абсолютно індивідуальна. Її повнота й дієвість багато в чому залежать від наявної в державі законодавчої бази, матеріально-технічних і фінансових ресурсів, що виділяє керівник підприємства, розуміння кожним зі співробітників важливості забезпечення безпеки бізнесу, а також від знань і практичного досвіду начальника системи економічної безпеки, що безпосередньо займається побудовою й підтримкою самої системи.

Лише незначна частка підприємств виділяє такий підрозділ як система економічної безпеки, частіше за все цими питаннями займаються менеджери, аналітики, охорона підприємства. Побудова системи економічної безпеки підприємства повинна здійснюватися на основі дотримання принципів [20]: законності прав і свобод громадян, конфіденційності, комплексного використання сил і коштів, передової матеріально-технічної оснащеності, корпоративної етики, координації й взаємодії з органами влади.

До основних елементів системи економічної безпеки підприємства належать [21]: захист комерційної таємниці й конфіденційної інформації, комп'ютерна безпека, внутрішня безпека, безпека будинків і споруд, фізична безпека, безпека зв'язку, безпека господарсько-договірної діяльності, безпека перевезень вантажів та осіб, безпека рекламних, культурних, масових заходів, ділових зустрічей і переговорів, протипожежна безпека, екологічна безпека, конкурентна розвідка, інформаційно-аналітична робота, техніко-технологічна безпека, кадрова безпека, виробнича безпека, фінансова безпека, податкова безпека, силова безпека.

**1. Зміст інформаційно-аналітичної діяльності: загальні поняття та визначення**

Існує багато визначень поняття "інформаційно-аналітичної діяльності". Поширеними є такі, що спрямовані на сферу управління. Фахівці розглядають інформаційно-аналітичну діяльність як процес у сфері управління, що являє собою процес пошуку, збору, переробки та подання інформації у формі, придатній для її використання; як інформаційно-аналітичну роботу у двох аспектах - інформаційну роботу та аналітичну роботу; як системне отримання, аналіз та накопичення інформації з елементами прогнозування з питань, що стосуються діяльності установи (Кулицький С. П., Кузнєцов І. М., Степанов Є. А. та Корнєєв І. К., Конотопов П. Ю., Курносов Ю. В. та інші).

Так, І. М. Кузнєцов у своєму підручнику "Информация: поиск, анализ, защита: Учебник по информационно-аналитической работе" розглядає інформаційно-аналітичну діяльність у двох аспектах, тобто розгалужує на інформаційну та аналітичну роботу (див. рис. 1).

До засобів інформаційної роботи автор відносить "сукупність документальних, технічних та інших пристроїв, призначених для накопичування, оброблення, систематизації, зберігання і видачі інформації".

Засобами аналітичної роботи І. М. Кузнєцов вважає закони і методи розумової діяльності, а також інші технічні засоби, на основі і за допомогою яких здійснюється обробка фактичних даних з більш високою якістю.



Рис. 1. Складові ІАД

Таким чином, технологія аналітичної роботи передбачає одержання нового знання (вивідної інформації), яке забезпечує складний процес дослідження.

Враховуючи різні підходи до визначення інформаційно-аналітичної діяльності по відношенню до будь-якої управлінської сфери, сформовано наступне узагальнене визначення: інформаційно-аналітична діяльність - це сукупність інформаційних процесів (збір, пошук, переробка інформації), необхідних для якісного та ефективного процесу управління.

Збір, обробка, використання та передача інформації є невід'ємним елементом успішної діяльності як підприємницької, так і будь-якої іншої. Будь-яке підприємство функціонує в системі ринкових відносин, причому характер цих відносин виходить за межі контактів з покупцями, постачальниками, торговими посередниками тощо. На діяльність підприємства впливають також науково-технічні, політичні, економічні та інші фактори. Тобто, результати діяльності підприємства визначаються тим, наскільки підприємство інформаційно забезпечено щодо впливу цих факторів.

На думку фахівців, прогрес людства у сфері інформаційної діяльності проявився у скороченні часу на передачу, обробку повідомлень і підготовку інформації для прийняття управлінських рішень; прогрес людства нерозривно пов'язаний з інтенсифікацією інформаційних процесів. Оскільки інформаційна діяльність, яка проявлялася у зниженні вартості обробки та передачі повідомлень, створювала умови для кращої організації матеріального виробництва та життєдіяльності суспільства в цілому.

Поняття "інформаційно-аналітична робота" розглядається як складова інформаційно-аналітичної діяльності. Під час проведення ІАД виділяють два рівні (або напрями) інформаційно-аналітичної роботи (ІАР):

1) інформаційний рівень, що полягає в пошуку, збиранні, зберігання, поширенні інформації;

2) аналітичний рівень, що полягає в узагальненні, класифікації інформації, її аналізі і перетворенні, розробці висновків, пропозицій, рекомендацій і прогнозів.

З позицій прийняття рішень розрізняють оперативний, тактичний, стратегічний рівні ІАР. Основними формами ІАР є: 1) моніторинг, що включає інформаційні зведення та огляди; 2) аналіз ефективності прийняття рішень; 3) дослідження актуальних проблем (інформаційні розробки, оперативні дослідження, аналітичні дослідження).

Основні принципи та методологічні аспекти інформаційно-аналітичної роботи: 1) формування мети досліджень; 2) створення понятійного апарату; 3) забезпечення достатньої інформованості; 4) розкриття значення фактів; 5) встановлення причин та наслідків; 6) врахування історичного розвитку та національного характеру; 7) визначення тенденцій розвитку; 8) забезпечення високого рівня достовірності; 9) формування висновків та рекомендацій; 10) наявність зворотного зв'язку.

Основні принципи аналітичної роботи:

1) цілеспрямованість - орієнтація аналітичної діяльності на досягнення конкретних цілей для вирішення певних завдань, як результатів практичної діяльності;

2) актуальність - аналітична діяльність повинна відповідати потребам практики, мати високій ступінь важливості на даний момент, в даній ситуації, для вирішення конкретної проблеми;

3) активність - проведення ІАД і видача її результатів незалежно від конкретних запитів користувачів з елементами прогнозування;

4) достовірність - врахування достовірності вихідних даних аналізу, точності кількісних даних, що використовуються, ступеня об'єктивності та обґрунтованості висновків, оцінок, пропозицій;

5) повнота - використання всієї наявної інформації, що має відношення до вирішення поставлених завдань;

6) альтернативність - наявність у кожного працівника аналітичного підрозділу можливості вільно висказати свою незалежну думку щодо результатів проведеного дослідження та довести її до вищого керівництва;

7) обґрунтованість - отримання аргументованих результатів аналітичної роботи на підставі сучасних досягнень науки, ефективних інформаційно аналітичних технологій тощо;

8) системність - комплексний аналіз проблем з урахуванням їх місця, ролі та взаємозв'язків в загальній структурі забезпечення діяльності установи;

9) своєчасність - отримання та видача результатів ІАД в потрібні терміни, у зручній формі та вигляді, що придатна для користування;

10) ініціативність - визначення та опис проблем, формування завдань і способів їх рішення (в т.ч., що виходять за межі традиційних уявлень);

11) об'єктивність - відсутність тенденційності, неупереджене відношення аналітика до дослідження та його результатів;

12) неперервність - організація постійно діючого інформаційно-аналітичного моніторингу обставин, своєчасне відображення основних змін в ситуації, що досліджується;

13) гнучкість - можливість швидкої адаптації до змін суспільно політичних обставин без модифікації структури методів і засобів реалізації аналітичної роботи.

Методологія аналітичних досліджень - це сукупність принципів, методів, способів та підходів до організації та проведення досліджень: принципи - вироблені наукою та практикою, сформульовані у концентрованому вигляді найбільш важливі ідеї, установки; метод - сукупність прийомів та способів пізнання; прийом - окрема дія для досягнення мети дослідження; спосіб - система дій, що застосовуються при виконання певного дослідження; процедура - встановлений порядок виконання прийомів та способів дослідження; методика - послідовність конкретних процедур, реалізація яких забезпечує досягнення мети досліджень; технологія (техніка) аналітичного дослідження - сукупність прийомів та способів, які входять до складу процедур.

Засоби ІАР - сукупність інтелектуальних та технічних засобів, що забезпечують виконання поставної мети.

Інтелектуальні засоби ІАР включають: відомості - характеристики властивостей об'єкту, що спостерігається або досліджується, представлені у доступній формі для людини; дані - факти або відомості, представлені у формалізованому вигляді, що забезпечує можливість їх зберігання, обробки та передачі; повідомлення - форма подачі інформації - сукупність логічно пов'язаних відомостей, що представляють для споживача єдине ціле.

Технічні засоби ІАР включають: інформаційні картки, каталоги, щоденники, інформаційні та інформаційно-аналітичні системи, системи інформаційного обслуговування, системи штучного інтелекту, експертні системи, АРМ аналітиків тощо.

Інформаційно-логічна система - система, що здатна вирішувати не лише пошук інформації, яка є у наявності, а й отримання інформації шляхом використання правил логічного висновку та умовиводів. Системи штучного інтелекту - автоматизовані системи, що моделюють інтелектуальну діяльність людини: лінгвістичні, процесори, навчаючи системи, експертні системи, Сі ДІР.

Фахівці називають основними професійними рисами керівника "аналітичність мислення, здатність до прогнозування ситуацій і результатів діяльності"; "здатність відбирати, систематизувати, аналізувати та узагальнювати інформацію"; "здатність розкласти проблему на складові частини, визначити і чітко сформулювати головні в даний період діяльності системи, визначити значущість кожного із змінних факторів, умов, проміжних результатів і таким чином здійснити комбінацію складових елементів з метою прийняття рішення з даної проблеми; здатність до дослідження протиріч у спостережуваних фактах, співставлення різних явищ і до виявлення характеру зв'язку між цими явищами".

Серед п'яти ключових компетенцій менеджера виділяють: інформаційну компетенцію (здатність побудови ефективної системи інформаційних ресурсів, необхідної для формування інформаційно-правової основи прийняття управлінських рішень; здатність визначення затребування певного інформаційного ресурсу в межах оперативного та стратегічного управління організацією) та аналітичну компетенцію (здатність обумовленої оцінки ефективності запропонованої для використання системи інформаційних ресурсів; здатність об'єктивної оцінки позитивних та негативних аспектів кожного компоненту системи інформаційних ресурсів; здатність здійснення оперативної аналітичної оцінки інформаційних потоків, отриманих від кожного компоненту інформаційної системи; уміння оперативно й ефективно здійснювати аналітичне співставлення інформаційних потоків, що виходять від кожного компонента системи інформаційних ресурсів; здатність формулювання на основі отриманої інформації комплексних аналітичних висновків; здатність інтерпретувати, систематизувати, критично оцінювати і використовувати отриману інформацію в контексті вирішуваного управлінського завдання або проблеми).

Для менеджера-аналітика важливими є процеси одержання, накопичування, обробки і передавання інформації, оскільки:

- інформаційно-аналітична діяльність дозволяє зібрати дані в цілісну картину про те, що відбувається, й спрогнозувати на перспективу дії різних факторів, структур, груп інтересів;

- аналітична діяльність забезпечує інформацією всі етапи управлінського циклу, підготовку, прийняття управлінських рішень і контроль за їх реалізацією;

- інформаційно-аналітична робота забезпечує стадії визначення проблем системи управління та їх аналіз; підготовку та прийняття управлінського рішення; контроль за його виконанням та оцінку його ефективності.

Таким чином, інформаційно-аналітична робота виявляється важливою складовою праці управлінського персоналу, є передумовою прийняття ефективних управлінських рішень.

**2. Організація інформаційно-аналітичної роботи в системі фінансово-економічної безпеки суб’єктів господарювання**

Перехід до ринкової економіки обумовив появу в українському законодавстві, юридичній та економічній літературі ряду нових понять, таких як комерційна таємниця, ділова інформація, секрет виробництва, торговельний секрет, ноу-хау, конфіденційна інформація, інформація обмеженого доступу.

Ці поняття можна об'єднати найбільш вживаним терміном - комерційна таємниця. Закони України "Про інформацію", "Про захист від недобросовісної конкуренції", "Про банки і банківську діяльність", "Про захист економічної конкуренції" та інші, а також ГКУ та ЦКУ регулюють спеціальний правовий режим охорони комерційної таємниці та інших видів інформації, пов'язаної з необхідністю захисту законних інтересів суб'єктів підприємницької діяльності. Вказані та інші законодавчі акти, спрямовані на розвиток правил чесної конкуренції, в той же час забороняють вторгнення в сферу чужих технологічних та комерційних секретів недозволеними методами. Вони дають підприємствам підґрунтя для створення правових систем захисту комерційної таємниці, які дозволяють організувати охорону відомостей, які складають комерційну таємницю, що належать їм. Одночасно вказані та інші закони України містять правові основи відшкодування підприємствам матеріальної та моральної шкоди, яку можуть заподіяти підприємству своїми неправомірними діями конкуренти, персонал підприємства, представники контрольноспостережних та інших органів державної влади і управління. З метою захисту своїх законних прав та інтересів щодо захисту комерційної таємниці суб'єкти господарювання можуть на законодавчій основі створювати систему захисту комерційної таємниці підприємства.

Мотивами порушення питання про створення такої системи можуть бути: досягнутий підприємством високий рівень науково-виробничої діяльності, виконання будь-яких унікальних робіт, надання кваліфікованих послуг, поява нових технологій на основі "ноу-хау", оригінальні комп'ютерні програми, розроблені стратегічні програми розвитку підприємства, планування рекламних заходів і т.ін., що потребують застосування захисних режимних заходів. Ще одним мотивом створення правової системи захисту комерційної таємниці повинно бути чітке розуміння керівником підприємства, що без створення такої системи будь-які юридичні претензії до недобросовісних конкурентів, клієнтів, штатних співробітників підприємства, посадових осіб органів державного управління виявляться безпідставними і не будуть мати юридичної сили. Накопичений практичний досвід свідчить, що підготовку до створення системи правового захисту комерційної таємниці підприємства слід починати зі здійснення поглибленого аналізу всієї господарської, науково-виробничої, фінансової, управлінської, маркетингової та іншої діяльності підприємства. Виходячи з досвіду захисту секретів західними фірмами, можна рекомендувати здійснити такий аналіз шляхом відповідей на питання, які містяться у зразку анкети підприємства-конкурента з виділенням також інформації, яка може класифікуватись як секретна.

До проведення аналізу доцільно залучати найбільш кваліфікованих робітників всіх структурних підрозділів підприємства: наукових співробітників, економістів, інженернотехнічний склад, менеджерів, маркетологів, фінансистів, юристів і т.ін. Важливо, щоб документ, підготований за результатами аналізу, найбільш повно віддзеркалював "обличчя" підприємства, розкривав його місце на ринку, перспективи розвитку та слугував переконливою основою для організації роботи по створенню на підприємстві системи правового захисту комерційної таємниці.

Після проведеного детального аналізу діяльності підприємства та в залежності від його результатів керівник підприємства на основі Закону "Про інформацію", Закону "Про банки і банківську діяльність" може прийняти рішення про встановлення режиму доступу до інформації ділового, професійного, виробничого, банківського та іншого характеру, яка може бути віднесена, на підставі зазначених законів, до категорій "комерційна таємниця", "банківська таємниця", "конфіденційна інформація". Теоретичні розробки спеціалістів в галузі захисту інформації В. М.Чаплигіна, В. А.Рубанова, Е. Солов'йова (Російська Федерація), І. Давидова, А. А. Чернявського, Г. О. Андрощука, П. П. Крайньова, Г. К. Нікіфорова, С. С. Нікіфорова (Україна), Л. Хофмана (США), Ж. Бержьє (Франція), а також практика збереження секретів західними фірмами інформації обмеженого доступу свідчить про те, що основними елементами та складовими системи правового захисту комерційної таємниці є:

1. Юридичне закріплення в основоположних документах підприємства: статуті, засновницькому та колективному договорах, правилах внутрішнього трудового розпорядку права на комерційну таємницю. Основою для юридичного закріплення права підприємства на комерційну таємницю є положення, що містяться в ГКУ, ЦКУ, законах України "Про інформацію", "Про колективні договори та угоди", а також Кодексі законів про працю України.

2. Визначення відомостей, які підлягають захисту як комерційна таємниця, розробка переліку таких відомостей, затвердження його як офіційного нормативного документа підприємства, доведення його до відома персоналу підприємства, який має безпосереднє відношення до цих відомостей за посадою чи характером виконуваної роботи. Основою для визначення відомостей, які будуть захищатись як комерційна таємниця, є також положення, що містяться в ГКУ, ЦКУ, законах України "Про інформацію", "Про колективні договори та угоди", Кодексі законів про працю України.

3. Якісний підбір персоналу підприємства для роботи з відомостями категорії "комерційна таємниця", виховання та навчання співробітників у зв'язку з їх роботою з такого роду інформацією, підготовка для них методичних положень, інструкцій, пам'яток, пов'язаних з поводженням з комерційною таємницею, створення матеріальних і моральних стимулів, що спрямовані на збереження комерційної таємниці.

4. Визначення порядку допуску та доступу до комерційної таємниці підприємства його співробітників, представників органів державного управління, партнерів, клієнтів, отримання від них юридичних документів, які зобов'язують їх на правовій основі зберігати комерційну таємницю. Ця вимога базується на конституційних положеннях, законах про органи виконавчої влади ("Про національну поліцію", "Про службу безпеки України") та інших.

5. Встановлення порядку збереження комерційної таємниці при укладанні господарських та інших підприємницьких договорів, а також ведення ділових переговорів, відвідання підприємства перед укладенням договорів. Цей елемент систем захисту комерційної таємниці базується на вимогах ЦКУ, ряді указів Президента України, постанов Кабінету Міністрів України, міжнародних договорах України.

6. Створення на підприємстві відповідно до закону "Про інформацію" порядку поводження з інформацією обмеженого користування, який виключає можливість витоку інформації при роботі з комерційною таємницею, при розробленні рекламних матеріалів, при веденні співробітниками ділових переговорів, під час наукових конференцій, семінарів, виступів у пресі. Даний елемент системи правового захисту комерційної таємниці повинен враховувати вимоги законів "Про інформацію", "Про науково - технічну інформацію", "Про основи державної політики в сфері науки і науково-технічної діяльності".

7. Визначення порядку взаємодії підприємства з представниками правоохоронних органів, контрольно-спостережних органів виконавчої влади, які на законодавчій основі можуть мати доступ до комерційної таємниці при виконанні ними своїх службових завдань та функцій. Даний елемент системи правового захисту комерційної таємниці повинен будуватися з урахуванням вимог законів: "Про місцеве самоврядування в Україні", "Про національну поліцію", "Про прокуратуру", "Про службу безпеки України" та інших.

8. Організація спеціального діловодства документів категорії "комерційна таємниця". Цей елемент системи захисту комерційної таємниці регулює порядок роботи та поводження з такими документами, їх підготовкою, обліком, розмноженням, пересиланням, зберіганням, періодичною перевіркою їх наявності та знищення. Викладені елементи та складові системи правового захисту комерційної таємниці повинні бути задіяні та використані в повній єдності та взаємодії. Якщо хоча б одна із складових викладеної вище системи не буде задіяна, то система не виконає свого призначення, оскільки може статися витік відомостей, які складають комерційну таємницю, та підприємство може втратити юридичні підстави для підняття питання про відшкодування нанесених конкурентом або персоналом підприємства матеріальних збитків.

**3. Суть інформаційно-аналітичної діяльності та її роль у формуванні ефективної системи економічної безпеки суб’єктів підприємництва**

Від якості інформаційно-аналітичного забезпечення прямо залежить якість управління економічною безпекою підприємства. Інформаційно-аналітичне забезпечення системи управління економічною безпекою підприємства повинне включати такі підсистеми: інформації, систем показників, індикаторів та методів оцінки та аналізу економічної безпеки підприємства.

Найбільш значуща властивість інформації – це здатність викликати зміни. Неодмінною умовою виживання в умовах ринку й збереження конкурентоспроможності є адаптація до мінливих потреб ринку та забезпечення економічної безпеки підприємства. Практично цінність інформації прямо пропорційна тій ролі, яку вона відіграє в прийнятті управлінських рішень. Цінність інформації визначається тим, як суб’єкт зможе розпоряджатися нею. Інформація, покликана забезпечити прийняття рішень, вносить істотний вклад у прийняття управлінського рішення. Вона стає фактором виробництва й подібно праці, матеріалам і капіталу дозволяє створювати додану вартість, тому інформація є критерієм забезпечення економічної безпеки підприємства.

Основними властивостями інформації є: повнота, вірогідність, цінність, актуальність і ясність.

Аналітичну обробку інформації дуже важливо здійснювати на основі системного підходу, що дозволяє розкрити комплексність об'єкта, багатогранність зв'язків і звести їх у єдину цілісну систему. Під системою в цьому випадку розуміється набір елементів і інформаційні зв'язки, що виникають між ними і які забезпечують оптимальне безпечне управління економікою підприємств.

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

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

2. системності – встановлення порядку функціонування всієї системи аналітичної інформації в цілому та її динамічних тенденцій;

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

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

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

6. принцип стандартизації – при створенні аналітичних комплексів повинні бути раціонально застосовані типові уніфіковані й стандартизовані елементи, проектні рішення, пакети прикладних програм;

7. принцип ефективності – полягає у досягненні раціонального співвідношення між витратами й цільовими ефектами;

8. принцип єдиної інформаційної бази – інформація вводиться один раз в систему і може бути використана багаторазово.

До збору, накопичення й систематизації інформації пред'являються певні вимоги: інформація повинна бути повною й своєчасною, достовірною, корисною й зручною для сприйняття й подальшого використання.

Систематизацію й підготовку джерел інформації для аналізу можна розділити на два етапи: перевірка їх змісту; обробка й вивчення матеріалів.

Процес підготовки матеріалу до аналізу економічної безпеки підприємства включає також приведення показників у порівнянний вид і спрощення цифрового матеріалу. Однорідність і порівнянність даних – обов'язкова умова одержання правильних результатів при проведенні економічного аналізу.

У процесі аналізу виявляються переваги й недоліки інформації, повнота її використання для аналізу й управління економічною безпекою.

Інформаційна база економічної безпеки, яка існує на підприємстві, становить систему показників, вірогідність, періодичність поновлення, повнота й автоматизація якої забезпечує якість прийнятих управлінських рішень. Система показників для проведення фундаментальних аналітичних досліджень економічної безпеки повинна враховувати такі вимоги до їх формування:

1. у систему повинні входити декілька окремих (частинних) показників і один узагальнюючий, залежний від частинних;

2. для системи повинна бути характерною інтегрованість, що дозволяє застосовувати її при програмно цільовому управлінні економічною безпекою й будувати «дерево» цілей економічного й соціального розвитку підприємства;

3. наявність достатньої кількості показників для оцінки окремих функціональних складових економічної безпеки підприємства;

4. усі показники в системі повинні бути реальними й динамічними;

5. можливість одержання прогнозу про спрямованість динаміки показників;

6. показники повинні бути значимими (найбільш важливими для дослідження економічної безпеки).

Доцільність формування ефективної системи економічної безпеки суб’єктів підприємництва зумовлена необхідністю постійної концентрації зусиль на зменшенні негативного впливу зовнішніх (нестабільність та невизначеність політичної та соціально-економічної ситуації в державі, часте коригування правового забезпечення, нерівномірний доступ до інформації, корупція тощо) та внутрішніх загроз. При цьому, варто відмітити, що в організації ефективної системи економічної безпеки суб’єктів підприємництва визначальне місце відводиться інформаційно-аналітичній діяльності.

Причина цього полягає у природному виборі найбільш раціональних та ефективних механізмів гарантування безпеки, а також у можливості їхнього застосування в конкретному випадку. Будь-які дії з організації безпеки можна відобразити в межах двох протилежних стратегій: реакції та превенції. Реактивний підхід припускає наступну схему розвитку подій: шкідлива дія - опір (стійкість) - компенсація.

Реактивний підхід є абсолютно необхідним, однак за своєю природою є надзвичайно витратним і небезпечним, оскільки спочатку допускає шкідливу дію, а вже потім - компенсаційну реакцію (в найкращому разі). Цілком очевидно, що реактивний підхід варто залишати на крайній випадок, коли не спрацьовує політика превенції. В ідеалі, підприємству слід прагнути отримувати випереджальну інформацію, завдяки якій можна вже на далеких підступах розпізнавати реальні загрози та заздалегідь обходити або нейтралізувати їх.

Формування ефективної системи економічної безпеки суб’єктів підприємництва передбачає застосування найуспішнішої стратегії досягнення стану безпеки, тобто - зміщення центру ваги зусиль у бік превенції та зниженні питомої ваги суто реактивних дій.

Аналізуючи взаємозв’язок категорій безпека й інформація, загальним висновком є очевидна необхідність ефективної інформаційно-аналітичної діяльності, що включає отримання великого обсягу якісної інформації як ззовні, так і з внутрішнього середовища, її якнайшвидше опрацювання й виявлення оптимальних, з погляду безпеки, варіантів поведінки. Змістом роботи із забезпечення економічної безпеки суб’єктів підприємництва є системна, раціонально організована, випереджальна та агресивна інформаційно-аналітична діяльність, проваджувана специфічними засобами.

Інформаційно-аналітична діяльність – це діяльність служби безпеки суб’єкта підприємництва щодо збору, систематизування, аналізу, узагальнення, оцінки вхідної інформації, яка надходить з різноманітних джерел та підготовка аналітичної (вихідної) інформації, яка містить оцінку поточної ситуації та прогноз її розвитку, для керівників підприємства. Виходячи із суті інформаційно-аналітичної діяльності виділяють два її рівні:

1. Інформаційний рівень, зміст якого зводиться до пошуку, збирання, накопичення, зберігання та поширення інформації.

2. Аналітичний рівень, що полягає в узагальненні, класифікації інформації, її аналізі і перетворенні, розробці висновків, пропозицій, рекомендацій і прогнозів.

Отже, варто розрізняти сам аналітичний процес (аналітику) та інформаційну діяльність.

Аналітичний процес – це процес аналізу існуючої інформації та створення нового знання, це робота інтелекту. Результатом аналітичної діяльності є вторинні документи, що є інформаційною моделлю не первинного документа, а моделлю проблеми.

У свою чергу інформаційна діяльність – це обслуговування аналітичного процесу (матеріальне, оперативно-технічне, архівне тощо). Критичний аналіз літературних джерел [1-3] дозволяє визначити аналітичну роботу (процес) у формуванні економічної безпеки суб’єктів підприємництва як сукупність дій, що відбуваються в інтересах підвищення ефективності управлінської діяльності і мають на меті пізнання сутності, причин, тенденцій розвитку подій і явищ в сфері безпеки підприємств, розгляд і оцінювання ситуацій, вироблення на основі аналізу й обробки інформації висновків, рекомендацій, прогнозів.

Дефініція інформаційно-аналітичної діяльності дозволяє констатувати, що вона є основою інформаційно-аналітичного забезпечення безпеки суб’єктів підприємництва.

Головною метою інформаційно-аналітичного забезпечення безпеки підприємництва є своєчасне викриття на ранній стадії заходів безпосередньої підготовки певних сил для нанесення економічних збитків підприємству, установі або організації та забезпечення відповідних їм дій, а також добування необхідної інформації для планування, підготовки і проведення заходів з метою недопущення можливих дій [2].

На практиці інформаційно-аналітичне забезпечення безпеки підприємництва виконується з метою виявлення схем недобросовісної конкуренції, шахрайства, обману у сфері бізнесу, задля використання їх для виключення потрапляння власної організації у ситуації некерованого ризику [1].

Таким чином, під інформаційно-аналітичним забезпеченням безпеки діяльності підприємства ми розуміємо цілеспрямовану взаємодію людського інтелекту (аналітика) і наявної вхідної інформації (відкритої та/або конфіденційної) з метою отримання споживачем інформації нового вивідного знання, що сприяє прийняттю оптимальних управлінських рішень. Критичний аналіз літературних джерел [1-3] дозволив виділити ряд етапів інформаційно-аналітичної діяльності:

1. Загальне знайомство із проблемою, за результатами якого складається загальний план роботи.

2. Визначення термінів та понять для ясності та однозначності представлення результатів.

3. Збір фактів.

4. Тлумачення фактів – максимальне визначення їх значення. Етап включає оцінку, класифікацію та аналіз фактів.

5. Побудова гіпотези. Гіпотезу можна розглядати як положення, яке полегшує прояснення проблеми, розкриває зв’язок між фактами.

6. Висновки. На цьому етапі приводяться докази або заперечення робочих гіпотез, які висуваються на попередньому етапі і робляться відповідні висновки.

7. Унаочнення. Складення документу в ясній, наочній та доступній формі. Вказується ступінь достовірності кожного твердження, готуються таблиці, діаграми тощо.

Об’єктом інформаційно-аналітичної діяльності є оперативна обстановка, тобто економічна ситуація, сукупність факторів, які безпосередньо або опосередковано впливають на стан, розвиток і результати суспільних відносин, визначають напрямки розвитку оперативної обстановки, форми, методи та засоби, які застосовуються. Зміст інформаційно-аналітичної діяльності полягає у приведенні різноманітних відомостей в логічно обґрунтовану систему залежностей (причинно-наслідкових, просторово-часових тощо), яка дає змогу дати правильну оцінку сукупності фактів та окремих фактів. Інформаційно-аналітична діяльність безсумнівно є широкою і багатогранною сферою діяльності. Її головною метою є отримання максимальної користі з фактів, які є в розпорядженні аналітика, для того щоб правильно зрозуміти і оцінити ситуацію, бачити її у перспективі, а в кінцевому підсумку – успішно діяти.

Весь інтерес роботи полягає у тому, що використовується величезний набір методів, які успішно застосовують в математиці, логіці. Інформаційно-аналітична діяльність – це процес, в результаті якого сирі факти перетворюються в довершену продукцію, передбачену для передачі замовнику. Адже, будь-яка кількість фактів, оброблених найкращим чином, занесених в досьє, проіндексованих, - не має жодної цінності, поки ми не розкриємо їх зміст, співставимо між собою і передамо іншим у тому вигляді, в якому їх значення буде абсолютно ясним.

Основним результатом інформаційно-аналітичної діяльності є вивідна (аналітична) інформація відображена у формі доповіді, інформаційної довідки або наукової праці, де подаються висновки та рекомендації. Вони абсолютно необхідні, для того щоб робота мала завершений вигляд і могла бути максимально корисною. Висновки є наслідком досягнення поставленої цілі. Щоб зробити висновки потрібно відповісти на питання “Що означає дане явище?”. В багатьох документах читаються і запам’ятовуються лише висновки, тобто результати аналізу. Необхідно виявляти якомога більшу турботу про те, щоб у висновках викладались коротко і чітко найважливіші моменти, але водночас стислість не повинна породжувати неправильне сприйняття. Написання висновків потребує найвищої майстерності фахівця. Отже, рівень безпеки підприємства тісно корелює з його рівнем інформаційно-аналітичної діяльності, тобто з його інформаційною захищеністю і його спроможністю добувати інформацію, а також, не меншою мірою - з його здатністю витримувати шкідливу дію в рамках реактивного підходу.

**Висновок**

Розвиток підприємства на всіх рівнях управління потребує відповідного інформаційно-аналітичного забезпечення. Одним із важливих завдань, що потребують нагального вирішення, є вдосконалення інформаційно-аналітичної діяльності процесів розвитку підприємства. Недосконалість інформаційно-аналітичної діяльності ускладнює і сповільнює обґрунтування та вибір конкретних напрямів господарського розвитку, збільшує ймовірність помилок, що є основною причиною низької ефективності сучасного бізнесу та незахищеності від дій конкурентів. Рівень безпеки підприємства тісно корелює з його рівнем інформаційно-аналітичної діяльності, тобто з його інформаційною захищеністю і його спроможністю добувати інформацію, а також не меншою мірою – з його здатністю витримувати шкідливу дію в рамках реактивного підходу. Перспектива подальших досліджень у цій галузі полягає в обґрунтуванні методології здійснення інформаційно-аналітичної діяльності для забезпечення економічної безпеки суб'єкта підприємництва.

**Завдання для самостійної роботи**

1. Історія виникнення та розвитку інформаційно-аналітичної діяльності.

2. Суть та основні принципи інформаційно-аналітичної діяльності.

3. Методи аналітики, їх універсальність в процесі пізнання.

4. Специфіка аналітики в системі сучасних наук: проблеми і перспективи.

**Питання для самоконтролю**

1. Основні принципи побудови системи економічної безпеки підприємства.

2. Розкрийте основні завдання системи економічної безпеки підприємства.

3. Наведіть основні елементи системи економічної безпеки підприємства.

4. Дайте характеристику системі економічної безпеки підприємства.

**Список рекомендованої навчальної, наукової, фахової і періодичної літератури:**

1. Позднишев Є. В. Інформаційно-аналітичне забезпечення безпеки підприємництва (методи та їх застосування) навч. посібник / Є. В. Позднишев. – Кн. 1. – К.: Видавець Позднишев, 2007. – 89 с.

2. Чергенець Е. В. Інформаційно-аналітичне забезпечення безпеки підприємництва (збір та пошук інформації) [Електронний ресурс] / Е. В.Чергенець, А. В.Зайцев, Є. В. Позднишев // Навчальний посібник. Книга 2 / Під заг. ред. Є. В.Позднишева. - К., Видавець Позднишев, 2007. - 74 с.

3. Ткачук Т. Ю. Конкурентна розвідка: навч. посіб. / Т.Ю. Ткачук. – К.: Наук.-вид. відділ НА СБ України, 2010. – 219 с.