МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Кафедра фінансово-економічної безпеки та інтелектуальної власності

Олійник Павло Павлович

Організаційно-правові аспекти управління системою фінансово-економічної безпеки підприємства / Organizational and legal aspects of financial and economic security system management of the enterprise

спеціальність: 8.18010014 – Управління фінансово-економічною безпекою
магістерська програма – Управління фінансово-економічною безпекою

Магістерська програма

Виконав студент групи ФЕБм-21
П.П. Олійник
_____

Науковий керівник:
к.ю.н., доцент, Н.Б. Москалюк
_____

Магістерську роботу допущено
до захисту:
«____» _____20___р.
Завідувач кафедри
_____ Н.Б. Москалюк

ТЕРНОПІЛЬ – 2017

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Економічний розвиток нашої держави, як і усіх інших держав, напряму залежить від стабільності функціонування підприємств та збільшення їх економічного потенціалу в умовах новітньої ринкової економіки. Глобалізація, як процес всеохоплюючий і незворотній, крім позитивних тенденцій справляє на суб'єктів господарювання і негативний влив у вигляді загроз та ризиків безпеці. Отож, в умовах господарювання перед підприємствами постає завдання захистити найважливіші інтереси, забезпечити сталий розвиток підприємства, своєчасно виявляти, запобігати і нейтралізовувати реальні та потенційні загрози. Саме із вказаною метою підприємство приймає рішення про створення власної служби безпеки або залучення найманих осіб для виконання вказаного завдання. Досвід свідчить, що середнім та великим за кількістю працівників підприємствам, а також всеукраїнським та міжнародним за статусом підприємствам, доцільним є створення власної служби безпеки із утриманням необхідної кількості високопрофесійних працівників у штатному розписі.

Україна як держава, в якій лише друге десятиліття формуються умови для функціонування ринкової економіки, не може похвалитися великим багажем науково-практичних досліджень у напрямку діяльності служб безпеки підприємств. До того ж, спеціальність «Управління фінансово-економічною безпекою» лише нещодавно введена до навчальних планів ВНЗ України, що зумовило відсутність комплексних наукових досліджень впливу служби безпеки підприємств на забезпечення стабільності фінансово-економічної безпеки суб'єкта господарювання.

Правовий статус у нормах національного законодавства вказаних служб потребує значного доопрацювання. Останні зміни, як то вступ України до СОТ чи підготовка до євроінтеграційних процесів, також вносять свої корективи у напрями можливого розвитку служб безпеки та шляхів

управління ними. Все вищезазначене підтверджує актуальність, новизну та практичну цінність проведеного нами дослідження.

Підґрунтям для проведеного дослідження стали праці таких національних та іноземних вчених як О. В. Ареф'єва, Н. І. Баяндин, І. Березин, І. А. Бланк, Боббі Майямей, Ю.В. Бондарчук, С. В. Васильчак, Войцех Конащук, В.М. Геєць, Л.І. Донець, З.Б. Живко, Д.В. Зеркалов, М.І. Камлик, Ю.Р. Кіньов, А.Н. Линниченко, О. М. Ляшенко, В.П. Мак-Мак, І. Мартиненко, А.І. Марущак, І. Нежданов, В.Л. Ортинський, Н.Й. Реверчук, Л.І. Скібіцька, А.А. Фастенко, А.О. Чередниченко, В.І. Ярочкін та інших. Варто зазначити, що праці названих вище вчених стосуються лише окремих аспектів діяльності служб безпеки підприємств, або ж є комплексними, проте відображають не національну теорію і практику їх діяльності. Отож, раціональність у проведенні нами дослідження на обрану тематику є незаперечною.

Метою дослідженняє комплексний аналіз усіх аспектів організації та управління службою безпеки підприємства; виявлення проблем у діяльності таких служб та обґрунтування можливих шляхів їх вирішення.

Для досягнення мети дослідження необхідно було виконати наступні **завдання:**

- охарактеризуватипоняття та складові системи безпеки підприємства;

- проаналізувати правовий статус служби безпеки підприємства за нормами національного законодавства;

- дослідити основні функції служби безпеки підприємства та механізм їх здійснення;

- - проаналізувати організаційні та правові аспекти створення служби безпеки підприємства;

- - провести науково-практичний аналіз принципів та етапів управління службою безпеки підприємства;

- - дослідити національну та іноземну практику структурної організації служби безпеки підприємства та завдання, які вирішуються кожним із

підрозділів;

- охарактеризувати бенчмаркінг як передумову вдосконалення всієї системи безпеки підприємства і роль служби безпеки у ньому.

Об'єктом дослідженняє система суспільних відносин, які складаються у процесі організації та управління службою безпеки підприємства.

Предметом дослідження є проблеми та перспективи організації та управління службою безпеки підприємства.

Методологія дослідження.Методологічною і теоретичною основою дослідження були загальнометодологічні методи пізнання: діалектичний, аналізу і синтезу, системний і конкретно-історичний підходи, порівняльний аналіз, структурно-функціональний аналіз та інші.

Інформаційною основою послужили національні, іноземні та міжнародні нормативно-правові акти, дані офіційної статистики, експертні оцінки, а також монографії, наукові статті вітчизняних та закордонних вчених, матеріали наукових конференцій тощо.

В результаті дослідження сформульовано та обґрунтовано низку наступних положень, що відрізняються науковою **новизною**:

Вперше:

- дано авторське визначення поняття безпеки, під яким пропонується розуміти стан об'єкта у динамічному середовищі з погляду здатності його до стійкості та розвитку в умовах загроз різного роду;

- обґрунтована необхідність законодавчої заборони службам безпеки підприємства займатись оперативно-розшуковою діяльністю та промисловим шпигунством з метою забезпечення безпеки суб'єкта господарювання;

- доведена нераціональність закладення основних функцій служб безпеки підприємств у законодавчий акт, оскільки виникнення нових загроз потребуватиме негайного їх відвернення, що може перешкодитися невчасним внесенням змін та доповнень до законодавства;

- запропоновано створення всеукраїнської бази даних по бенчмаркінгу, яка міститиме інформацію про усіх суб'єктів господарювання, що бажають взяти участь у вказаному процесі, що зніме проблему пошуку партнерів.

Набули подальшого розвитку:

- висновок про необхідність законодавчого врегулювання правового статусу служби безпеки підприємства через прийняття окремого законодавчого акту, сфера дії якого поширюється виключно на суб'єктів господарювання;

- теза про необхідність встановлення законодавчої норми, що Служба безпеки не має права виконувати завдання в інтересах третіх осіб на договірних основах;

- думка про те, що недоцільним є використання досвіду таких країн як Російська федерація, Чеська республіка, Польща та інші, які законодавчо передбачають необхідність прийняття Статутів служб безпеки суб'єктів господарювання. З цього приводу висловлюється позиція необхідності поміщення окремого розділу, який стосуватиметься діяльності служб безпеки у загальний Статут підприємства.

Практичне значення одержаних результатів. Матеріали та висновки дослідження можуть бути використані: 1) у правотворчості під час опрацювання пропозицій щодо змін та доповнень до норм цивільного та господарського законодавства; 2) у практичній діяльності суб'єктів господарювання; 3) у навчальному процесі під час викладання курсів «Організація та управління майновою та особистою безпекою підприємств», «Теорія організації», «Правові основи організації та функціонування системи економічної безпеки», «Сучасні методи забезпечення надійності персоналу» та інших.

Апробація результатів дослідження. Результати дослідження булиапробовані на Всеукраїнській науково-практичній конференції, в ході якої було опубліковано тези доповіді на тему «Бенчмаркінг як передумова до вдосконалення системи безпеки підприємства» // Матеріали збірника тез

доповідей всеукраїнської науково-практичної конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави. – Тернопіль, 2016. – С. 111-113.

Структура магістерської роботи. Роботаскладається з вступу, чотирьох розділів, шести підрозділів, висновків, переліку використаних джерел та додатків. Повний обсяг роботи становить 100 сторінок друкованого тексту. Перелік використаних джерел містить 96 найменувань і викладений на дев’яти сторінках.

РОЗДІЛ 1. СЛУЖБА БЕЗПЕКИ В ОРГАНІЗАЦІЙНІЙ СТРУКТУРІ ПІДПРИЄМСТВА

1.1. Поняття та складові системи безпеки підприємства

Під час створення підприємства і визначення організаційної його структури перед засновниками виникає раціональне питання щодо забезпечення його безпеки. Зважаючи на мету такого захисту приймається одне із наступних рішень: якщо захисту потребують лише матеріальні цінності або фізичне життя і здоров'я працівників, то доцільним є залучення на комерційній основі працівників ліцензованих охоронних структур; якщо ж загрози носять комплексний характер і шкода, яка може бути спричинена підприємству є великою або особливо великою, то необхідне створення власного підрозділу служби безпеки підприємства із необхідним правовим, ресурсним та організаційним забезпеченням.

Важливо, що усвідомлення комплексності загроз може спостерігатися у засновників не одразу в момент створення підприємства, а вже після виходу його на ринок. Значно гірше, якщо таке усвідомлення приходить після завдання шкоди підприємству, адже усунення наслідків її часто перевершує матеріальне забезпечення, що потрібне було для створення органу, який би вчасно відвернув загрозу.

Та, незважаючи на те, коли прийшло усвідомлення необхідності створення власної служби безпеки, важливо, щоб воно все-таки прийшло. І коли таке усвідомлення існує, починається самий цікавий з наукової точки зору процес – процес організації вказаної служби і визначення шляхів управління нею. Чому цей процес є цікавим? Та тому, що саме від того наскільки якісно і раціонально буде побудована служба безпеки підприємства, настільки ефективною буде система безпеки підприємства. До того ж, єдиної уніфікованої форми створення і управління службою не існує, а тому кожне підприємство методом спроб і помилок будує власну систему

безпеки. І якраз вивчення всього багатоманіття національних та іноземних служб безпеки дозволяє винести науково-обгрунтовані висновки щодо можливих шляхів покращення їх діяльності.

Системне уявлення щодо необхідності забезпечення безпеки підприємства дозволяє усвідомлено і цілеспрямовано проводити роботу щодо такого забезпечення всіма його підрозділами й співробітниками. При цьому провідна роль служби безпеки не зникає, навпаки, розуміння своєї ролі і місця в системі безпеки підприємства призведе тільки до позитивних результатів.

Повертаючись до аналізу поняття та складових системи безпеки підприємства, слід підкреслити, що на сьогоднішній день немає єдиного підходу до визначення поняття «система безпеки підприємства». Кожен із науковців висловлює власне бачення на це поняття. Ми ж для визначення досліджуваного поняття пропонуємо попередньо виявити елементи системи безпеки підприємства. Вивчення великої кількості наукової літератури та документів практики дозволили намдійти висновку, що найлогічнішою видається структура, запропонована російським вченим Мак-маком В.П. Так, вчений до структурних елементів системи безпеки підприємства відносить: наукову теорію його безпеки, політику і стратегію безпеки, засоби та методи забезпечення безпеки і, нарешті, концепцію безпеки підприємства [61]. Вказана позиція, на наш погляд, відзначається логічністю, обґрунтованістю та вичерпністю.

Важливо, що лише у комплексі усі вказані елементи являтимуть собою завершену систему безпеки підприємства.

Наукова теорія безпеки підприємствазнаходиться в Україні на стадії формування. Відноситься це насамперед до понятійного апарату . Розглянемо детальніше деякі із понять.

Так, поняття безпеки окремо не міститься в жодному нормативно-правовому акті України, проте його можна виділити із поняття національна безпеки, що наведено у ст . 1 Закону України «Про основи національної

безпеки України» від 19.06.2003 року. Отож, під національної безпекою Закон пропонує розуміти: «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам…» [39]. Розкриття вказаного поняття через термін « захищеність », на нашпогляд, значно звужує її зміст. Сутність безпеки, на нашу думку, пов'язана із активними діями по забезпеченню стійкості і постійного розвитку. У зв'язку з цим під окремим поняттям безпекинами пропонується розуміти стан об’єкта у динамічному середовищі з погляду здатності його до стійкості та розвитку в умовах загроз різного роду.

Під загрозою безпеці підприємства необхідно розуміти потенційно або реально можливу подію або явище, які здатні порушити його стійкість і розвиток або призвести до зупинки його діяльності. Загрози можна класифікувати по різних підставах і вимірювати їх у кількісних параметрах. Доволі поширеною у науковій літературі є класифікація загроз за ступенем ймовірності загроза. За вказаною класифікацією загрози можуть бути: неймовірні, малоймовірні, ймовірні, вельми ймовірні і цілком ймовірні[42, с. 17].

Кожна із загроз за ступенем розвитку проходить чотири етапи: виникнення, експансію, стабілізацію і ліквідацію[45, с. 102]. Віддаленість загрози у часі визначається як безпосередня, близька (до 1 року) і далека (понад 1 рік), а віддаленість у просторі - територія підприємства, прилегла до підприємства територія, територія регіону, територія країни, зарубіжна територія [47, с. 31]. Темпи наростання загрози вимірюються по місяцях, кварталах, роках. Крім цього, загрози діляться за природою їх виникнення на два класи:1) природні (повені, землетруси і т.п.), 2) штучні (викликані діяльністю людини).

За характером загрози поділяють на економічні, соціальні, правові, організаційні, інформаційні, екологічні, технічні кримінальні та інші.

Метою забезпечення безпеки підприємства є комплексний вплив на потенційні і реальні загрози, що дозволяє йому успішно функціонувати в нестабільних умовах зовнішнього і внутрішнього середовища [51, с. 13].

Для досягнення вказаної мети необхідна ідентифікація загроз для стабільності й постійного розвитку підприємства і опрацювання заходів протидії виявленим загрозам.

Система безпеки підприємства є комплексним поняттям і включає в себе такі підсистеми як: економічну, інформаційну, кадрову, екологічну,науково-технічну,психологічну, фізичну, пожежнубезпеку тощо.

Важливо, що вищевказані підсистеми можуть включати в себе власні підсистеми. До прикладу, підсистемами економічної безпеки можуть бути майнова, фінансова, комерційна, та інші.

Крім цього, поділ на підсистеми є доволі умовним, оскільки кожна із них не існує окремо від інших, а лише у взаємозв'язку з ними. Поділ єдиної системи безпеки підприємства на підсистеми різних рівнів проводиться виключно з науково-методичних міркувань, оскільки це дозволяє більш детально аналізувати всі його елементи і нічого не залишити поза увагою.

Ефективність функціонування системи безпеки підприємства оцінюється завдяки такому критерію як ступінь відсутності або наявності завданої йому шкоди.

Політика безпеки підприємства як одна із складових системи безпеки покликана визначати загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цілей. Важливо, що для встановлення загальних орієнтирів необхідно спочатку сформулювати цілі забезпечення безпеки підприємства. Такими цілями, на думку Т.Б. Кузенко, можутьбути:

- Зміцнення дисципліни праці і підвищення його продуктивності;
- Захист законних прав та інтересів підприємства;
- Зміцнення інтелектуального потенціалу підприємства;
- Збереження та примноження власності;
- Підвищення конкурентоспроможності виробленої продукції;

- Максимально повне інформаційне забезпечення діяльності підприємства і підвищення його ефективності;

- Орієнтація на світові стандарти і лідерство в розробці та освоєнні нової технології і випускається;

- Виконання виробничих програм;

- Надання сприяння управлінським структурам у досягненні цілей підприємства;

- Недопущення залежності від випадкових і несумлінних ділових партнерів [56, с. 142].

Отож, загальними орієнтирами, які є підґрунтям політики безпеки, можуть бути:

- зміцнення ресурсного потенціалу;

- здійснення комплексних превентивних заходів щодо підвищення рівня захищеності майна і персоналу підприємства;

- залучення у діяльність по забезпеченню безпеки підприємства усіх його підрозділів;

- продумана і виважена кадрова політика підприємства;

- пріоритетмирних та законних методів запобігання і нейтралізації загроз.

Для успішного впровадження політики необхідно сформувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства [61].

У науковій літературі сформовано наступні типи стратегій безпеки:

1) орієнтовані на усунення існуючих або запобігання виникнення можливих загроз;

2) націлені на запобігання впливу існуючих або можливих загроз на предмет безпеки;

3) спрямовані на відновлення (компенсацію) завдається шкоди [66].

Як бачимо, перші два типи передбачають таке забезпечення безпеки, в результаті якого загроза не відбувається або вона не здійснює впливу на безпеку підприємства.В останньому випадку шкода допускається, проте вона компенсується діями, які передбачені відповідною стратегією. Звісно, стратегія третього типу реалізується виключно у випадках, коли немає змоги застосувати перші два типи, або ж шкода є непомірно меншою, ніж ціна заходів на її відвернення.

Реалізацією заходів із забезпечення безпеки підприємства займаються суб'єкти, яких можна розділити на дві групи.Суб’єкти першої групи займаються вказаною діяльністю безпосередньо на підприємстві і підпорядковані його керівництву. Серед суб’єктів досліджуваної групи можна виділити спеціалізовані суб'єкти (рада або комітет безпеки підприємства, служба безпеки), основним призначенням яких є постійна професійна діяльність щодо забезпечення безпеки підприємства. Іншу частину суб'єктів цієї групи умовно можна назвати напівспеціалізованою, оскільки частина функцій цих суб'єктів призначена для забезпечення безпеки підприємства (юридичний, фінансовий відділ і т.д.). До третьої частини цієї групи суб'єктів належить увесь інший персонал підприємства, які в рамках своїх посадових повноважень зобов'язані вживати загальних заходів до забезпечення безпеки підприємства.

До другої групи суб'єктів відносяться органи та організації, що функціонують самостійно і не підпорядковуються керівництву підприємства, але при цьому їх діяльність має суттєвий вплив на безпеку підприємства. Суб'єктами другої групи є:

1) Законодавчі органи. Прийняті на рівні держави закони складають правову основу діяльності щодо забезпечення безпеки підприємства.

2) Органи виконавчої влади. Прийняті на рівні цих органів підзаконні акти багато в чому доповнюють, уточнюють, деталізують норми законів.

3) Суди. Судові органи забезпечують дотримання законних прав та інтересів підприємства, в т.ч. у сфері безпеки.

4) Правоохоронні органи. Такі органи здійснюють боротьбу з правопорушенням, які негативним чином впливають на стан безпеки підприємства.

5) Науково-освітні установи, що покликані забезпечити науково-методичне опрацювання проблем безпеки підприємства та підготовку відповідних фахівців у сфері безпеки підприємств.

Для здійснення функцій із забезпечення безпеки підприємства суб'єкти повинні володіти певними засобами і методами забезпечення такої безпеки.

Серед існуючих засобів забезпечення безпеки на сьогоднішній день використовуються: технічні, організаційні, інформаційні засоби, фінансові та кадрові кошти, правові та інтелектуальні засоби тощо. Слід зауважити, що застосування кожного з вищевказаних засобів окремо не дає необхідного ефекту, він можливий тільки на комплексній основі. У той же час необхідно відзначити, що одночасне використання всіх вищевказаних коштів в принципі неможливо [69, с. 71].

Після аналізу всіх вищевказаних елементів системи безпеки підприємства необхідно перейти до складання концепції безпеки. Як відомо, концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем [73, с. 24].

Для того, щоб концепція безпеки виконувала поставлені завдання, необхідно аби вона виконувала такі вимоги як конструктивність, вписуваність та відкритість.

Вищевказані вимоги диктують, на думку Н.О. Подлужної, в якості обов'язкової умови включення в логічну структуру концепції наступних позицій:

1) Виявлення об'єкта і предмета, визначення їх сутності, місця серед безлічі інших.

2) Чітке формулювання ролі реалізації концепції і завдань, що стоять при її реалізації.

3) Виділення умов, необхідних і достатніх для реалізації концепції, і зіставлення їх з реально існуючими.

4) Визначення кола заходів, що забезпечують перетворення об'єкта реалізації концепції, а також шляхів її реалізації.

5) Формулювання критеріїв успішності заходів щодо розробки концепції, а також з оцінки результатів її реалізації [75, с. 5].

Концепція безпеки підприємства працює лише тоді, коли вона являє собою офіційно затверджений документ, в якому відображена система поглядів, вимог і умов організації заходів безпеки персоналу і власності підприємства.

Отож, сформована на науковій основі та охарактеризована нами вище система безпеки підприємства є організаційною основою створення її структурного підрозділу - служби безпеки. Правовий же статус вказаної служби визначається нормами чинного національного законодавства України. Важливо зазначити, що лише у поєднанні належно врегульованого правового статусу та мудрого організаційного супроводу система безпеки підприємства в змозі виконувати поставлені на неї завдання.

1.2. Правовий статус служби безпеки підприємства за нормами національного законодавства

Протидія загрозам і ризикам, які впливають на безпеку суб’єкта господарювання та підприємницьку діяльність в цілому потребує від персоналу підприємства не лише спеціальних умінь та навичок, а й докладної правової регламентації. І якщо для охоронної діяльності на сьогодні існують певні правові нормативи, викладені у Законі України «Про охоронну діяльність», то права та обов’язки служб безпеки суб’єктів господарювання не визначені ні на рівні закону, ні на рівні підзаконного нормативно-правового акта.

Встановлене дозволяє стверджувати, що діяльність служб безпеки у вказаній ситуації може здійснюватися за аналогією права та аналогією закону. Тобто, до діяльності вказаного підрозділу можуть застосовуватися норми чинного цивільного та господарського законодавства, які визначають загальні засади здійснення підприємницької діяльності. І якщо особливих проблем із регламентуванням штатних розписів, посадових інструкцій та робочого часу не виникає, то питання повноважень у розслідуванні порушень, які відбулись на підприємстві, володіння та застосування зброї, доступу до інформаційних джерел тощо потребують обов'язкової регламентації на рівні закону. Наголошуємо, що навіть визначення вказаних питань на підзаконному рівні не вирішить означених проблем, оскільки застосування норм вищої юридичної сили завжди ставитиме під загрозу повноваження керівника чи співробітників служби безпеки підприємства.

Цікаво, що спроби визначити правовий статус служб безпеки підприємств в Україні уже були, проте і до нині вони не завершились успіхом. З метою вироблення власних рекомендацій щодо правової регламентації правового статусу відповідних служб, вважаємо за необхідне коротко проаналізувати зареєстровані у Верховній Раді України законопроекти, які стосуються означеного питання.

12 січня 2004 року депутати Верховної Ради України розглядали комплекс законопроектів щодо детективної та охоронної діяльності. Два з них стосувалися узаконення детективної діяльності і носили назви „Про приватну детективну діяльність" та „Про детективну діяльність", інші два – охоронної діяльності - проект Закону „Про службу безпеки суб'єктів господарювання та інших юридичних осіб" і проект Закону „Про охоронну діяльність". Як обґрунтовували автори законопроектів, в Україні вже довгий час проводиться діяльність окремих фізичних та юридичних осіб, які містить ознаки детективної, проте їх діяльність не регламентується жодними нормативно-правовими актами. Те ж саме стосувалося і охоронної діяльності.

Ситуація на сьогоднішній день з правовою регламентацією охоронної діяльності змінилася, оскільки відповідний закон було все-таки прийнято. Та, як вказувалося вище, він жодним чином не стосується діяльності служб безпеки суб'єктів господарювання, а тому і застосовуватись у визначенні правового статусу вказаних служб не може.

30 березня 2006 року у Верховній Раді було зареєстровано проект Закону «Про служби безпеки суб'єктів господарювання» за № 9264, спрямований на визначення правових, організаційних та управлінських основ функціонування служб безпеки суб'єктів господарювання, порядку їх взаємодії з іншими суб'єктами, які здійснюють діяльність по забезпеченню безпеки, прав, обов'язків і гарантій служб безпеки у зв'язку із здійсненням цієї діяльності.

Аналізом саме останнього законопроекту і порівняння його норм із попередніми ми і займемося.

По-перше, уваги потребує назва законопроекту – «Про служби безпеки суб'єктів господарювання». На відміну від попереднього законопроекту «Про службу безпеки суб'єктів господарювання та інших юридичних осіб», вона видається значно логічнішою. Обґрунтувати правильність такої позиції можна тим, що «іншим юридичним особам», тобто некомерційного призначення недоцільно утримувати власну службу безпеки. Їх некомерційна спрямованість вилучає із системи безпеки таку її складову як фінансово-економічна безпека. Для забезпечення безпеки масових заходів чи фізичної охорони споруд та майна таких юридичних осіб економічно доцільніше буде наймати спеціальні охоронні структури, правовий статус яких чітко регламентований на законодавчому рівні.

Цікаво, що на такій же позиції стоїть і російський законодавець, який у Законі Російської Федерації «Про охоронну та детективну діяльність» прямо вказує на те, що «Під підприємством, яке має право засновувати власну службу безпеки розуміється виключно комерційна організація» [61, с. 13].

У законопроекті 2006 року пропонувалося закласти безмежно велике число основних завдань служби безпеки. До речі, вказаний перелік доволі схожий із переліком, що містився у законопроекті 2004 року. Варто наголосити на тому, що вказаний перелік беззаперечно може бути поміщений у посадову інструкцію працівника служби безпеки підприємства уже сьогодні, навіть без прийняття закону. Адже ніхто не відміняв принципу «Дозволено все, що не заборонено законом». Значно більше уваги потребує, на нашу думку, визначення дій, які не можуть вчинятися представниками служби безпеки. Так, необхідно зважати на вимогу закону, що оперативно-розшукову діяльність можуть здійснювати виключно обмежена кількість державних органів. Проведення ж оперативно-розшукової діяльності іншими підрозділами чітко встановлених органів, підрозділами інших міністерств, відомств, громадськими, приватними організаціями та особами забороняється.

Цікавими з позиції суперечності до вимог чинного законодавства є наступні пункти законопроекту 2006 року:

- «служба безпеки відповідно до своїх завдань зобов'язана: 4) виявляти, запобігати, припиняти та розкривати злочини, вживати з цією метою профілактичних та інших заходів, передбачених чинним законодавством (*прим. авт. – якщо із першими трьома позиціями ми ще можемо погодитись, то четверта викликає у нас щире подивування, оскільки суперечить нормі щодо суб'єктів оперативно-розшукової діяльності*);5) припиняти адміністративні правопорушення на об'єкті (*норма сформульована, на нашу думку, невірно, адже якщо адміністративне правопорушення відбулося, то логічним завершенням його є настання адміністративної відповідальності. Нагадаємо, що не лише притягувати до такого виду відповідальності не мають права працівники служби безпеки підприємства, а навіть складати протоколи про адмінправопорушення є незаконним*).

Отож, як бачимо, у законопроекті 2006 року на служби безпеки підприємств покладаються окремі функції, не притаманні підрозділам

суб'єктів приватного права, і які прямо віднесено до компетенції правоохоронних органів.

Не зовсім вірним видається нам і перелік прав, якими слід наділити служби безпеки за законопроектом:

- подавати запити до правоохоронних органів та отримувати відповіді на них відповіді у встановлені законодавством терміни (вказане право і на сьогоднішній день передбачено нормами чинного інформаційного законодавства України);

мати безоплатний доступ до інформаційних баз органів державної владиз метою забезпечення безпеки об'єкта (закріплення вказаного права прирівняло б у правовому статусі підрозділи безпеки із правоохоронними органами держави, що є недопустимим);

створювати детективні підрозділи та підрозділи охорони та приватного розшуку відповідно до поставлених завдань (вказане право є виключною прерогативою власника (співвласників) підприємства);

зберігати, носити і застосовувати спеціальні засоби та зброю відповідно до Закону України «Про міліцію» (закріплення названого права є найбільш проблематичним для співробітників служб безпеки підприємств, оскільки необхідні будуть зміни у всій дозвільній системі держави).

Усі інші права у переліку, поданому законопроектом цілком виправдані і не суперечать вимогам чинного національного законодавства.

В обох законопроектах міститься норма, яка безумовно впливає на правовий статус служби безпеки: «Службі безпеки забороняється виконувати завдання в інтересах третіх осіб на договірних основах». Таким чином визначається не лише підконтрольність служби безпеки, а й можливі сфери її діяльності. Ми стоїмо на позиції, що вказана норма обов'язково має міститись у законі, який надіємось у найближчому часі все-таки набуде юридичної сили.

Цікавою нормою законопроекту 2003 року є те, що співробітникам служби безпеки забороняється видавати себе за представників правоохоронних органів, здійснювати оперативно-розшукову, розвідувальну

контррозвідувальну діяльність, отримувати інформацію без особистої згоди громадян. Вказана норма є не зовсім логічною, оскільки практика діяльності відповідних служб у іноземних країнах чітко спрямовується на розвідувальні та контррозвідувальні заходи. Навіть у багатьох службах безпеки існують підрозділи із аналогічними назвами. Внесення вказаної норми у поданій редакції, на нашу думку, перекреслить усі можливості, та і мету діяльності служби. Доречнішим було б визнання незаконною діяльність служби із промислового шпигунства, елементи якого вже визнані кримінально-караними діяннями згідно норм чинного кримінального законодавства України.

Отож, виходячи із вищевказаного, можна констатувати гостру необхідність у прийнятті окремого законодавчого акту, який би врегулював основні засади, принципи діяльності та правовий статус служб безпеки підприємств. Виключно після цього можна буде говорити про можливості забезпечення безпеки підприємств, принаймні правової та організаційної її складових.

1.3. Основні функції служби безпеки підприємства та механізм їх здійснення

Види послуг, які службі безпеки дозволяється надавати своєму підприємству – засновнику законодавчо в Україні не визначені. Проте, можна, враховуючи досвід іноземних країн, визначити найбільш оптимальний список, який у подальшому можна було б презентувати до законодавчого акту у досліджуваній сфері.

Отож, основними функціями служб безпеки можна визначити:

1. Збір відомостей з цивільних справ на договірній основі з учасниками процесу.Вказана функція дозволяє виявити благонадійність контрагентів та їх фінансову культуру.

2. Встановлення обставин недобросовісної конкуренції з боку інших підприємств. Так, під недобросовісною конкуренцією розуміється

застосування в конкурентній боротьбі засобів і методів, пов'язаних з порушенням чинного законодавства, що регламентує виробничу і комерційну діяльність підприємств або норм і правил взаємовідносин між конкурентами, прийнятих на ринку товарів і послуг [66].

На сьогоднішній день відомі такі форми недобросовісної конкуренції:

• встановлення контролю над діяльністю конкурента з метою припинення цієї діяльності;

• встановлення дискримінаційних цін або комерційних умов;

• недобросовісна реклама;

• встановлення залежності поставок конкретних товарів або послуг від прийнятих обмежень відносно виробництва або розподілу конкуруючих товарів;

• введення обмежувальних умов у агентські угоди;

• таємну змову на торгах і створення таємних картелів;

• порушення якості, стандартів і умов поставок товарів і послуг;

• підробка і виробництво оригінальних виробів, що випускаються конкурентом;

• використання свого економічного потенціалу для продажу продукції за цінами нижче собівартості (демпінг) з метою підриву позицій конкурента і подальшого витіснення його з ринку;

• зловживання панівним становищем на ринку (наприклад, надмірне завищення цін або відмова здійснювати поставки);

• встановлення дискримінаційних комерційних умов;

• поширення неправдивих, неточних або перекручених відомостей, здатних заподіяти збитки господарюючому суб'єкту, чи завдати шкоди його діловій репутації;

• введення споживачів в оману щодо характеру, способу і місця виготовлення, споживчих властивостей, якості товару;

• некоректне порівняння господарюючим суб'єктом у процесі його рекламної діяльності, вироблених чи реалізованих ним товарів з товарами інших господарюючих суб'єктів;

• несанкціоноване придбання і використання фірмових секретів конкурента;

• самовільне використання товарного знака, фірмового найменування або маркування товарів;

• отримання, використання, розголошення науково-технічної, виробничої або торговельної інформації, у т.ч. комерційної таємниці, без згоди її власника.

3. Збір відомостей щодо кримінальних справ.

Кримінальні справи, до розслідування яких долучається служба безпеки, умовно можна розділити на дві групи: порушені у зв'язку з вчиненням злочинів проти персоналу підприємства і злочини проти власності засновника [46, с. 23].Якщо аналізувати злочини першої групи, то обов'язковою умовою збору відомостей про них є їх зв'язок з діяльністю підприємства-засновника. Наприклад, крадіжка особистого майна у співробітника фірми сама по собі не зобов'язує співробітників служби безпеки долучатися до розслідування цього злочину, однак, в тому випадку, якщо серед цього майна виявляться документи підприємства-засновника, то ситуація змінюється протилежним чином. Можливе підключення співробітників служби безпеки до розслідування кримінальних справ, за якими працівник підприємства є обвинуваченим у скоєнні злочинів, однак, робити це необхідно тільки за вказівкою або з дозволу керівника підприємства. До найбільш поширених злочинів другої групи відносяться крадіжки, грабежі, дрібні розкрадання, підпали і т.д.

Вельми актуальними для співробітників служби безпеки стали злочини у сфері економічної діяльності і проти інтересів служби в комерційних організаціях.

Закон допускає збір відомостей про скоєний злочин тільки після відкриття кримінального провадження. У той же час на практиці часто з'являється значний відрізок часу (іноді в кілька діб) між подією злочину, який став відомим правоохоронним органам і порушенням кримінального провадження. Видається більш раціональним, що в таких випадках служба безпеки повинна, не чекаючи порушення кримінального провадження, приступити до збору відомостей щодо скоєного злочину, одночасно направити при цьому в правоохоронний орган, що проводить перевірку, письмове повідомлення про скоєний злочин.

4. Розслідування фактів розголошення комерційної таємниці підприємства.

Під комерційною таємницею норми ст..505 Цивільного кодексу України пропонують розуміти інформацію, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [91].

Таким чином, будь-яка конфіденційна інформація, що представляє цінність для підприємства в досягненні переваг над конкурентами і отримання прибутку, може стати комерційною таємницею підприємства . Не вдаючись в методику визначення інформації, що становить комерційну таємницю відзначимо, що такою вона стає тільки після затвердження керівництвом підприємства «Переліку відомостей, що становлять комерційну таємницю підприємства»,оголошення його під розписку всім причетним до неї співробітникам і надання статусу комерційної таємниці конкретній інформації, що зафіксована на будь-яких матеріальних носіях.

Слід пам’ятати, що на законодавчому рівні визначається перелік відомостей, які не можуть бути визначені комерційною таємницею. До вказаного переліку віднесено:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;

- інформація за всіма встановленими формами державної звітності;

- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

- документи про сплату податків і обов'язкових платежів;

- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

- документи про платоспроможність;

- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

- відомості, що відповідно до чинного законодавства підлягають оголошенню [81, с. 106].

За фактом розголошення комерційної таємниці підприємства служба безпеки повинна проводити розслідування і передавати необхідні матеріали до суду для притягнення винних осіб до відповідальності.

5. Збір інформації про осіб, які уклали з підприємством контракти.

Підприємство зазвичай укладає два типи контрактів: комерційні та трудові. Одним з договірних умов може бути письмова згода особи, з якоюукладається контракт, на збір інформації про його біографічні та іншідані, що характеризують особу.

6. Пошук втраченого майна підприємства

Під майном підприємства розуміються матеріальні цінності, що знаходяться в його власності,оперативному віданні або корпоративному управлінні, грошові кошти в касі, на розрахунковому та інших рахунках у банках, нематеріальні активи (патенти, ліцензії, програми, ноу -хау, брокерські місця і т п.). У вузькому сенсі слова під майном підприємства розуміються речі (матеріальні цінності). Зміст роботи співробітників служби безпеки залежно від категорії втраченого майна носить різний характер, адже і способи незаконного заволодіння цим майном є доволі різними.

7. Розшук безвісти зниклих співробітників

Без вісті зниклою вважається особа, що зникла раптово, без видимих для того причин, місцезнаходження та доля якої залишається невідомою.

Всі випадки безвісного зникнення співробітників можна розділити на чотири групи:

• пов'язані з кримінальним характером сталося (вбивство, наїзд транспорту зі смертельним результатом і т.д.);

• зумовлені некримінальним позбавленням життя зниклого (самогубство, утоплення і т.д.);

• об'єктивно не залежать від свідомості і волі співробітників і не носять кримінальний характер (відхід з будинку внаслідок психічного захворювання, адміністративний арешт і т.д.);

• викликані проблемами особистого і службового характеру (сімейні негаразди, сварка з начальством і т.д.) [89].

Співробітники служби безпеки підключаються до розшуку безвісти зниклого співробітника тільки в тому випадку, якщо є підстави припускати, що його відсутність на роботі призведе (може призвести) до реальної чи потенційної шкоди підприємству. Діяльність служби безпеки з розшуку безвісти зниклого співробітника - це комплекс заходів, що здійснюються при тісній взаємодії з органами внутрішніх справ з метою встановлення фактичних обставин його зникнення і фактичного місцезнаходження.

8. Розслідування фактів неправомірного використання об’єктів інтелектуальної власності підприємства.

Найчастіше неправомірно використовуються комерційні найменування та торговельні марки підприємства, оскільки споживачі значно легше купують продукцію під відомою йому маркою, а для недобросовісних підприємців незаконне використання таких об’єктів скорочує витрати на розробку продукції і цим самим зменшує її собівартість. Таким чином, дії недобросовісних суб’єктів господарювання завдають значної шкоди підприємствам-власникам об’єктів інтелектуальної власності. І вказана шкода носить не лише матеріальний, а й нематеріальний характер (через порушення доброї ділової репутації).

Незаконне використання патентів на винаходи, корисні моделі та промислові зразки зустрічаються набагато рідше, оскільки для використання технологій, що підтверджуються патентом, необхідне спеціальне устаткування, яке є лише в обмеженої кількості суб’єктів господарювання. А тому, найчастіше підприємства, що володіють патентами і виготовляють на їх основі свої товари і послуги, знають про всіх можливих суб’єктів, що можуть незаконно використати запатентовані об’єкти.

9. Виявлення некредитоспроможних партнерів

Некредитоспроможним визнається той партнер, у якого для отримання кредиту немає передумов, що підтверджують здатність повернути його.Служба безпеки зобов'язана виявляти некредитоспроможних партнерів як до укладення, так і в процесі реалізації договору і своєчасно інформувати про це керівництво підприємства.

10. Виявлення ненадійних ділових партнерів

Ненадійність ділового партнера визначається:

• великою кількістю зірваних з його вини угод з іншими фірмами;

• невиконанням або неналежним виконанням умов укладених договорів;

• умисним затягуванням ділових переговорів;

• зневажливим ставленням до прав інтелектуальної власності;

• пред'явленням до нього значної кількості судових позовів;

• наявністю великого боргу;

• нетривкою позицією на ринку;

• нерегулярним і ненадійним постачанням сировини і товарів;

• відсутністю довіри з боку споживачів;

• зіпсованою репутацією серед ділових кіл.

Здатність служби безпеки своєчасно виявити хоча б окремі параметри ненадійності майбутніх або справжніх ділових партнерів в значній мірі може вплинути на ступінь економічної безпеки підприємства-засновника.

11. Вивчення негативних аспектів ринку.

Комплексний аналіз ринку проводить спеціально призначена для цього служба підприємства, яка поряд з офіційною економічною інформаціє, використовує відомості, представлені службою безпеки. Такі відомості можуть бути зведені у два блоки: 1) стан і вплив тіньової економіки на ринок і 2) кримінальні аспекти ринку .

12. Збір інформації для проведення ділових переговорів.

Основними стадіями переговорів є:

1. підготовка до переговорів;

2. процес їх ведення;

3. аналіз результатів переговорів і виконання досягнутих домовленостей [87, с. 140].

Співробітники служби безпеки беруть участь в зборі інформації на першій і другій стадіях. При всій умовності такого поділу служба безпеки повинна представляти на різних стадіях керівництву підприємства-засновника свою інформацію. Наприклад, в процесі підготовки до переговорів відомості про учасників майбутніх переговорів, їх сильні і слабкі сторони, їх позиції і плани ведення переговорів, підготовлені матеріали, конкурентоспроможність та платоспроможність ділового партнера і т.д.

Під час проведення переговорів служба безпеки повинна поставляти інформацію про зміни позиції партнерів по переговорах, про можливі спроби

з їх боку шантажувати, підкуповувати членів делегації підприємства-засновника, проведення розвідувальних заходів щодо їх і т.д. [81, с. 16].

13. Захист життя і здоров'я персоналу від протиправних посягань

Захист організовує служба безпеки або всього персоналу підприємства (під час виконання ним своїх професійних обов’язків), або деяких його категорій (керівники, касири і т.д.). При цьому чітко визначається час проведення охоронних заходів . Охоронці повинні бути націлені, насамперед на припинення насильницьких злочинів (замах на вбивство, пограбування) і адміністративних проступків (дрібне хуліганство) щодо осіб, які охороняються . Повинні широко застосовуватися технічні засоби захисту .

14. Забезпечення порядку в місцях проведення підприємством представницьких, конфіденційних та масових заходів

Залежно від типу заходів видозмінюється і зміст діяльності служби безпеки. Наприклад, при проведенні закритих нарад основна увага приділяється, насамперед, захисту відомостей, що становлять комерційну таємницю, на виставках необхідно вживати заходів до недопущення крадіжки або псування майна підприємства; при проведенні концертів основна увага приділяється фізичній безпеці людей і т.д. Для кожного із заходів службою безпеки обираються свої механізми та устаткування для забезпечення безпеки.

15. Консультування та надання рекомендацій керівництву і персоналу підприємства з питань забезпечення безпеки.

В обов'язки служби безпеки входить не тільки консультування і подання рекомендацій співробітникам підприємства з питань забезпечення безпеки, але і її реалізація. Проведення консультацій та рекомендацій з питань безпеки, зазвичай, не виходить за межі таких її основних видів, як економічна, інформаційна, пожежна, фізична безпека.

16. Проектування, монтаж та експлуатаційне обслуговування засобів охоронно-пожежної сигналізації.

Засоби охоронно-пожежної сигналізації призначені для виявлення спроб проникнення на об'єкт і виникнення пожежі, оповіщення співробітників служби безпеки про появу і наростання цих загроз та забезпечення контролю доступу на об'єкт, що охороняється . Діяльність підрозділу служби безпеки,у вказаному напрямі здійснюється в кілька етапів. Перший етап (проектування) передбачає планування робіт з впровадження та капітального ремонту засобів сигналізації, обстеження об'єкта з метою одержання вихідних даних для розробки виконавчої проектно-кошторисної документації; матеріально-технічне забезпечення монтажних робіт. Останній етап (експлуатаційне обслуговування) включає в себе:

• здачу цих засобів в експлуатацію;

• планування експлуатаційних заходів та контроль за їх виконанням;

• технічне обслуговування, технічний контроль за експлуатацією засобів сигналізації;

• ремонт приладів та апаратури охоронно-пожежної сигналізації;

• матеріальне забезпечення експлуатаційних потреб;

• ведення встановленої технічної документації;

• збір та узагальнення статистичних даних по експлуатаційно-технічного обслуговування;

• аналіз причин відмов у роботі апаратури і причин, що сприяють вчиненню крадіжок та пожеж з заблокованих ділянок об'єкта [77].

Короткий огляд основних функцій служби безпеки дозволяє стверджувати, що вони органічно взаємно доповнюють один одного і в разі їх успішної реалізації утворюють єдине «поле» безпеки підприємства-засновника. Лише вчасне і вміле застосування службою безпеки підприємства усіх можливостей захисту сприяють підтриманню безпеки на високому рівні.

Висновок до розділу 1.

При дослідженні служби безпеки в організаційній структурі підприємства, нами було детально розглянуто поняття та складові системи безпеки підприємства, правовий статус служби безпеки за нормами національного законодавства України, а також основні функції служби.

Аналіз поняття та складових системи безпеки підприємства дозволив нам сформувати позицію про відсутність єдиного розуміння поняття безпеки і законодавчого його забезпечення. Розгляд великої кількості наукової літератури привів нас до усвідомлення, що систему безпеки підприємства формують такі складові як політика та стратегія безпеки, суб'єкти безпеки підприємства, засоби та методи забезпечення безпеки, а також концепція безпеки. Лише у поєднанні вказані елементи створюють єдину дієву систему безпеки підприємства.

Правовий статус служби безпеки підприємства є на сьогоднішній день найменш опрацьованим і врегульованим питанням. Так, нам вдалось встановити, що жодний нормативно-правовий акт ні на рівні закону, ні на рівні підзаконного нормативно-правового акту не містить норм, які б визначали правовий статус служб безпеки суб'єктів господарювання. Безумовно, до служб безпеки можна застосовувати загальні норми цивільного та господарського законодавства, проте такі питання як спеціальні функції, володіння зброєю та її застосування, доступ до інформаційних масивів та баз даних потребують належного правового регулювання на рівні окремого законодавчого акту. Досвід іноземних держав у визначенні правового статусу служб безпеки підприємств показує, що певні оперативно-розшукові заходи та можливість використання зброї і спецтехніки віддано правоохоронними органами у руки працівників служб безпеки. Національні реалії при цьому докорінно відрізняються. Так, чинне законодавство України містить норму про виключну компетенцію спеціально встановлених органів державної влади у проведенні оперативно-розшукової

роботи. Доволі складною є процедура отримання дозволів на носіння зброї навіть для працівників суб'єктів господарювання, що отримали ліцензію на провадження охоронної діяльності. У жодному законодавчому акті навіть не згадується про можливість володіння зброєю працівниками служб безпеки підприємства, а це значно обмежує можливість виконання ними своїх безпосередніх завдань у сфері безпеки.

При аналізі правового статусу служб безпеки нами було опрацьовано ряд законопроектів, що реєструвалися у ВРУ, які були націлені на встановлення організаційних та правових аспектів діяльності вказаних підрозділів суб'єктів господарювання. Ґрунтовне дослідження представлених законопроектів дозволило сформувати нам власну позицію з приводу усіх складових правового статусу досліджуваних підрозділів підприємства.

Основні функції служб безпеки аналізувались нами на досвіді іноземних держав у цій сфері, оскільки і їх національне законодавство не передбачає. З приводу функцій, нами висловлена позиція, що вони мають бути передбачені не законодавчим актом, а локальним (на рівні підприємства), адже загрози можуть виникати щоразу нові і на них потрібно реагувати миттєво. Зміни ж до законодавчих актів приймаються проблематично і зі значною затримкою, що зумовлюватиме нові виклики для безпеки підприємства.

РОЗДІЛ 2. ПРАКТИКА ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ СЛУЖБОЮ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Створення служби безпеки підприємства: організаційні та правові аспекти

Ефективне функціонування служби безпеки передбачає попереднє опрацювання багатьох питань. Серед них особливого значення набуває проектування оргструктури служби безпеки та її ресурсного забезпечення, оскільки без вирішення цих питань її діяльність взагалі неможлива.

Загальновідомо, що будь-яке структурне формування створюється для реалізації певних функцій. Аналіз цих функцій, яки нами наводився у попередньому розділі дослідження, дозволяє стверджувати, що для їх реалізації необхідно, як мінімум, створити три підрозділи служби безпеки: розвідку, контррозвідку та охорону. Зрозуміло, кількісне співвідношення працюючих в них співробітників буде різним і воно носить доволі об'єктивний характер. Серед причин, що визначають нерівномірну кількість співробітників у різних підрозділах служби безпеки, можна назвати фінансові можливості підприємства-засновника, наявність або відсутність охоронюваних таємниць, ступінь участі в конкурентній боротьбі і т.д. Більше того, в практиці деяких служб безпеки зустрічаються випадки об'єднання двох детективних підрозділів (розвідка і контррозвідка) в один загальний. Таке об'єднання, хоча воно і має часто вимушений характер, не можна визнати вдалим. Основною причиною небажаності такого об'єднання є те, що кожен підрозділ служби безпеки має свої специфічні цілі, завдання та функції, реалізація яких (оскільки вони взаємно доповнюють і не суперечать один одному) дозволяє значно підвищити ефективність служби безпеки в цілому.

Звісно, кожен підрозділ підприємства має бути очолюваний керівником (начальником) служби безпеки. Цілком очевидно, що якщо персонал служби безпеки за кількістю великий, неминуче постає питання про заступників

начальника служби безпеки. Їх також повинно бути не менше трьох (за кількістю підрозділів служби безпеки), в крайньому випадку, двох, якщо існує єдина детективна служба.

Як правило, заступник начальника служби безпеки є одночасно керівником одного з підрозділів і, в свою чергу, також має одного або кількох заступників.

У великих службах безпеки можливе введення посад помічників (референтів) начальника. Слід зазначити, що в маленьких (за кількістю персоналу) службах безпеки проектування їх оргструктури на цьому можна і закінчити, затвердивши його у керівника підприємства-засновника.

Інша ситуація складається у великих службах безпеки, де виникає необхідність створення штабних підрозділів,оскільки начальники служби безпеки просто фізично не здатні на належному рівні виконувати такі управлінські функції, як аналіз, планування, контроль і т.д. Виконання цих обов'язків помічниками стан справ не змінює, тому що в цьому випадку виникає необхідність їх повсякденного керівництва, що знову-таки не під силу начальнику служби безпеки і він змушений буде призначити одного з них координатором діяльності інших, а це по суті означає виконання обов'язків начальника штабу. Слід зазначити, що створення штабу в структурі служби безпеки звичайно викликає заперечення керівників підприємства - засновника та подолання їх небажання є важкою справою. Запропонована схема організаційної структури повинна час від часу уточнюватися і переглядатися.

Будь оргструктура, навіть найоптимальніша, не зможе дати очікуваних результатів, якщо її не доповнити внутрішніми нормативними актами, що регулюють діяльність усіх підрозділів і співробітників служби безпеки. Вказані нормативні акти умовно можна розділити на дві групи: ті, що безпосередньо відносяться до діяльності самої служби безпеки і до діяльності інших служб (підрозділів, співробітників) підприємства. До першої групи науковці відносяться: Статут служби безпеки, Положення про відділи та

штаби служби безпеки, Положення про групи і сектори служби безпеки, посадові інструкції співробітників служби безпеки [79, с. 31].

Деяку непогоджуваність викликає у нас наявність у переліку актів такого документу як Статут служби безпеки підприємства. Ми вважаємо, що окремого статуту для підрозділу підприємства не потрібно, все необхідне може бути поміщене окремим розділом у Статут підприємства як цілісний документ, затверджений засновниками суб'єкта господарювання.

Положення про службу безпеки підприємства має не суперечити вимогам чинного законодавства України. Саме такий зразок положення буде наведено нами у додатку А до магістерської роботи.

Структура посадової інструкції повинна включати наступні розділи: загальні положення; функції; посадові обов'язки; права, відповідальність; взаємини і зв'язок за посадою. Розробка цих нормативних актів мати здійснюватись послідовно, починаючи з Статуту до посадової інструкції, що дозволяє охопити весь комплекс цілей, завдань і функцій, розв'язуваних службою безпеки.

Друга група внутрішніх нормативних актів, що забезпечують діяльність інших співробітників і служб підрозділів підприємства-засновника, включає в себе:

• договір підприємства з партнером про забезпечення ним заходів безпеки комерційної інформації;

• інструкцію для виконавців робіт і документів, що містять комерційну таємницю;

• зобов'язання про нерозголошення комерційної таємниці;

• перелік відомостей, що становлять комерційну таємницю підприємства та основні вимоги до співробітників щодо її захисту;

• перелік відомостей, які не повинні розголошуватися стороннім особам з метою особистої безпеки співробітників, підприємства;

• перелік посадових осіб, уповноважених відносити інформацію до комерційної таємниці;

• правила віднесення інформації до комерційної таємниці та зняття з їх носіїв грифу конфіденційності;

• правила ведення секретного діловодства;

• пам'ятку працівнику (службовцю) про збереження комерційної таємниці підприємства;

• правила прийому відвідувачів на підприємстві;

• правила внутрішнього трудового розпорядку і т.д [61].

Зрозуміло, всі ці нормативні акти розробляються співробітниками служби безпеки спільно з відповідними службами підприємства, і після їх затвердження керівництвом підлягають також спільному контролю за їх виконанням.

Однак оптимальна структурна побудова та повне правове забезпечення служби безпеки самі по собі не призведуть до її ефективного функціонування, якщо вона не буде забезпечена відповідними ресурсами. Серед них першорядне значення мають фінансові ресурси. Без фінансового забезпечення діяльності служби безпеки безглуздо взагалі говорити про її функціонування.

Оскільки служба безпеки не має права самостійно заробляти гроші шляхом укладення договорів з іншими клієнтами, саме на підприємстві-засновника лежить обов'язок фінансування її діяльності . Але це не означає, що керівництво служби безпеки має займати в цьому питанні пасивну позицію. Навпаки, обґрунтовані поточні та прогнозні оцінки у фінансових потребах служби безпеки і засновані на них точні розрахунки повинні стати правилом, а не винятком.

Фінансову політику служби безпеки визначають, звичайно, її керівники, але при цьому активну допомогу їм повинна надавати бухгалтерська служба.

У функції цієї служби входить:ведення табелю, обліку робочого часу; нарахування зарплати, премій; облік виплат за різні послуги; перерахування грошей;видача співробітникам їх грошового утримання;оплата рахунків і т.д.[66]

Не менш важливе значення для керівників служби безпеки має питання кадрового забезпечення її діяльності. Цю роботу умовно можна розділити на два етапи.

На першому етапі відбувається відбір кандидатів для роботи в службі безпеки, їх перевірка, проходження ними спеціальної підготовки і стажування на посаді. При відборі кандидатів особлива увага повинна приділятися їх освіти (крім юристів, доцільно запрошувати на роботу економістів, фінансистів і т.д.). Не завадить і з'ясування біографічних та інших даних, що характеризують особу кандидата .

Якщо в процесі перевірки встановлено придатність кандидата для роботи в службі безпеки, то його направляють на навчання (за винятком осіб, які мають стаж роботи в оперативних або слідчих підрозділах не менше трьох років).

Після зарахування співробітника на постійну роботу настає етап закріплення його на роботі в службі безпеки . Він складається з підвищення його професійного рівня, проведення роботи щодо зміцнення трудової дисципліни і законності, забезпечення правового і соціального захисту .

Відомо, що отримані спеціальні знання не завжди підкріплені відповідними вміннями та навичками. Тому закріплення й удосконалення цих навичок у працівниківмає приділятися основна увага.

Вельми актуальними є також питання про дотримання трудової дисципліни і законності, зміцнення фізичного розвитку, здоров'я, підвищення культури .

Повне і якісне забезпечення діяльності служби безпеки матеріально - технічними ресурсами - не тільки засіб, а й умова підвищення ефективності роботи його співробітників. Ці ресурси умовно поділяються на такі групи:

• зброю і боєприпаси;

• спеціальні засоби;

• службові приміщення різного характеру;

• допоміжна техніка (автотранспорт, відео-, кіно-, фото- техніка, засоби оперативного радіо - і телефонного зв'язку, комп'ютери і т.д.);

• засоби попередження і захисту (охоронно-пожежна сигналізація, сторожові собаки, охоронне освітлення, телебачення т.д.);

• засоби забезпечення нормальної діяльності співробітників (меблі, канцелярське приладдя, медикаменти, бланки документів, юридична та спеціальна література і т.д.).

Нагадаємо, що володінню вказаними ресурсами не присвячено жодної норми у законодавстві України, а тому питання залишається за межами закону.

Нарешті, останнє по рахунку, але не за важливістю, забезпечення діяльності служби безпеки інформаційними ресурсами .

Перш за все, слід визначити потребу і обсяги інформації, без яких функціонування служби безпеки взагалі неможливо. Таку інформацію можна умовно розділити на три блоки (« сферу функціонування підприємства», «стан безпеки всередині підприємства» та «внутрішньо організаційну діяльність служби безпеки »), після чого в рамках кожного блоку розробити перелік необхідних відомостей. Цей перелік не носитиме довільний характер, якщо при його складанні керуватися одним принципом: будь-яка інформація реально повинна «обслуговувати», «працювати» на реалізацію, як мінімум, однієї функції служби безпеки [51, с.32]. Можна рекомендувати в цьому зв'язку включати в вищевказані блоки такі відомості, які, зрозуміло, не можуть бути вичерпними.

Цілком очевидно, що без належної організації великого масиву інформації, зручної і практичної для використання, не обійтися. Ідеальним варіантом у цьому випадку було б створення інформаційної системи на базі комп'ютерної техніки.

Для ефективної роботи всієї системи безпеки на підприємстві визначальне значення має особистість керівника служби безпеки. Саме до

підбору належної кандидатури керівника слід підходити якомога виваженіше.

Так, при підборі керівника служби безпеки підприємства в більшості випадків на першому місці стоїть не питання професіоналізму, а питання лояльності. Адже в силу виконуваних функцій цій людині буде відомо не тільки все про компанію , але і всі проблемні місця в її роботі, весь негатив, а часом і дуже багато про приватне життя керівництва.Слід погодитися із тим, що зважитися комусь віддати цю інформацію дуже не просто. З іншого боку, керівник розуміє, що він змушений зробити цей вибір, і чим раніше це відбудеться, тим менше втрат буде у підприємства.

Широко поширена думка , що подібного кандидата необхідно шукати лише серед своїх і виключно серед колишніх співробітників правоохоронних органів. Це значно звужує і так вузьке коло можливих кандидатів. Звичайно , людина з рекомендаціями хорошого знайомого користуватиметься більшою довірою , ніж сторонній кандидат. Але свої, а тим більше родичі, в силу наявності зв'язку з керівником, впевнені в тому, що до роботи можнавідноситись абияк.

Те, що шукати співробітника потрібно серед вихідців із силових структур, також вимагає певного коментаря. Як правило, колишні співробітники , які пропрацювали в органах тривалий час, є професіоналами, але тільки в своїй спеціалізації. А керівник СБ повинен бути обізнаним у великій кількості питань. Крім того , професіоналів органи не відпускають , за ними спостерігають , їх можуть в будь-який момент залучити до співпраці, а це може становити лишній ризик для безпеки підприємства. Крім того , тривала робота у відповідних структурах накладає відбиток і на стиль життя , і на поведінку людини. А це певна специфіка , до якої не всі готові .

Останнім часом з'явилося достатньо фахівців в сфері забезпечення безпеки бізнесу побічно або взагалі ніяк не пов'язаних із силовими структурами. Так, їх не так багато , як хотілося б , але вони є, і витрати на їх

пошук і залучення до співпраці обов’язково окупляться достойними результатами.

Ще один аспект пошуку кандидата на посаду керівника служби безпеки полягає в чіткому розумінні цілей даного заходу. Необхідно перш за все відповісти на запитання: навіщо це потрібно? Які пріоритети в роботі створюваної служби безпеки ? Чи це потрібне для усунення загрози з боку конкурентів, чи для боротьбиіз шахрайством персоналу, чи протидії криміналу або нейтралізація впливу силовиків. Залежно від відповіді на поставлене питання і потрібно шукати фахівця . Якщо головна проблема - силовики, то потрібен виходець з керівних посад з цих структур з відповідними зв'язками . Якщо кримінал, то співробітник , який мав досвід роботи з ними і досвід створення відповідних систем безпеки. Якщо конкуренти - незамінний досвід збору інформації та аналізу економіки підприємств.

Отже, пошук кандидата на посаду керівника служби безпеки підприємства потрібно вести всіма доступними засобами, попередньо проконсультувавшись з фахівцями про те , що повинна знати така людина, про що його потрібно запитати , на що звернути увагу в бесіді .

2.2. **Науково-практичний аналіз принципів та етапів управління службою безпеки підприємства**

Паралельно зі створенням служби безпеки її керівникам доводиться вирішувати питання управлінського характеру. Причому, в процесі функціонування служби ці питання набувають все більшої актуальності. Пов'язано це з тим, що управління службою безпеки повинно бути ефективним, бо в іншому випадку їй загрожує ліквідація, оскільки підприємство - засновник не потерпить незадовільних (або посередніх) результатів такої діяльності [33, с. 26].

У цьому зв'язку на перший план виступають питання створення і підтримки на відповідному рівні основних елементів системи, механізму та процесу управління . Розглянемо їх докладніше .

Система управлінняскладається з суб'єкта, об'єкта управління, прямого і зворотного зв'язку. Суб'єктом управління службою безпеки виступають керівник підприємства,рада (комітет) безпеки підприємства та начальник служби безпеки. Успішно виконувати свої завдання ці суб'єкти можуть тільки в тому випадку, якщо компетенція кожного з них буде суворо визначена в локальних правових актах таким чином, щоб не виникалипідґрунтя для конфліктів. Якщо це зроблено досить успішно, то можна говорити про сформовану керуючу підсистему.

Об'єктом управління (керованої підсистемою) в службі безпеки виступають її окремі співробітники та підрозділи. Співробітниками можуть бути не тільки безпосередні працівники служби безпеки підприємства, а й інші громадяни, які працюють у допоміжних підрозділах.

Об'єкт управління пов'язаний із суб'єктом управління каналами прямого і зворотного зв'язку (інформаційними каналами) . По каналу прямого зв'язку інформація у вигляді управлінських рішень надходить від суб'єкта управління до об'єкта, а по каналах зворотного зв'язку - у зворотному напрямку, сигналізуючи про стан об'єкта управління, його реакції на управлінські впливи .

Саме управлінський вплив, в свою чергу, реалізується у формі таких функцій управління, як прогнозування, планування, організація, регулювання, мотивація і контроль [27, с. 4]. У системі управління всі ці функції об'єднані в цілісний процес, хоча з методичних міркувань доцільно розглядати їх окремо. Розглянемо вищевказані функції з урахуванням специфіки діяльності служби безпеки.

Прогнозування передбачає складання висновку (прогнозу) про майбутню подію, тенденції розвитку служби безпеки. Прогнозні оцінки бувають оперативними, короткостроковими, середньостроковими.

Складаються вони як залученими спеціалістами, так і співробітниками служби безпеки (в першу чергу співробітниками штабу).

Якість прогнозних оцінок підвищується, якщо вони складаються співробітниками служби безпеки за допомогою запрошених експертів-фахівців у тій чи іншій сфері.

Практика доводить, що найбільш доцільним є складання наступних видів прогнозних оцінок:

1. кримінологічні;

2. ризики (комерційний, фінансовий і т.д.) у підприємницькій діяльності;

3. економічна, фізична, інформаційна і т.д. безпека підприємства.

Планування передбачає визначення цілей, завдань служби безпеки на майбутній період діяльності, коштів і часу на їх досягнення. Найбільш поширеними в діяльності служб безпеки є комплексні та спеціальні плани.

Так, комплексні плани охоплюють всі сфери діяльності служби безпеки і включають в себе, як правило, такі розділи, як організаційні питання, забезпечення всіх видів безпеки підприємства (в рамках компетенції служби безпеки), робота з кадрами, ресурсне забезпечення, контроль і т.д.

Спеціальні плани розробляються на випадок виникнення надзвичайних подій та надзвичайних ситуацій (нападу на об'єкт, загроза вибуху бомби, захоплення заручників, повінь, пожежа тощо) [34, с. 215].

Відповідно, структура планів також повинна бути різною за умови адекватного реагування на ці події.

Функція організації складається у встановленні постійних і тимчасових взаємин між усіма підрозділами служби безпеки, визначення порядку та умов її функціонування. Це процес об'єднання сил і засобів для досягнення поставлених цілей. Такий процес складається з наступних елементів:

1 . Визначення раціональних форм поділу праці .

2 . Розподіл робіт серед працівників, груп працівників і підрозділів.

3 . Розробка структури органів управління .

4 . Регламентація функцій, підфункцій, робіт, операцій .

5 . Встановлення прав і обов'язків органів управління та їх співробітників.

6 . Підбір і розміщення кадрів [43].

Контроль складається в процесі порівняння фактично досягнутих результатів із запланованими. Ефективна система контролю повинна відповідати таким вимогам:

1 . контроль повинен бути всеосяжним;

2 . контроль слід зосередити на результаті;

3 . система контролю повинна бути простою;

4 . контроль не може бути ні цілеспрямованим, ні нейтральною;

5 . контроль повинен бути постійним.

Суб'єктами контрольної діяльності в службі безпеки є: керівник підприємства-засновника, члени ради (комітету) безпеки підприємства, керівники служби безпеки і його підрозділів (в рамках своєї компетенції) . Підконтрольними об'єктами можуть бути - діяльність підрозділів, стан технічного укріплення об'єкту, що охороняється, захищеність комерційної таємниці, система професійної підготовки та перепідготовки співробітників служби безпеки і т.д. Вибір об'єкта контролю визначається його здатністю впливати (позитивно або негативно) на діяльність служби безпеки в цілому. У рамках підконтрольного об'єкта дуже важливі його складові елементи, після визначення яких можна безпосередньо приступити до контролю.

На сьогоднішній день розрізняють три види контролю:

1 . попередній (здійснюється до фактичного початку робіт);

2 . поточний (здійснюється в ході здійснення робіт) та

3 . заключний (здійснюється після виконання робіт) [46, с. 23].

З урахуванням специфіки діяльності служби безпеки переважну увагу слід приділити попередньому і поточному контролю .

У механізмі управління мета є системоутворюючим елементом. Спочатку формулюється мета, а потім інші елементи механізму управління

службою безпеки. Формулювання мети залежить від багатьох факторів: фінансових можливостей підприємства-засновника, його географічного розташування, можливості набрати з числа жителів даної території кваліфікований склад співробітників служби безпеки і т.д.

На основі сформульованої мети проектується і створюється оргструктура служби безпеки. Аналіз вивчених документів служб безпеки свідчить, що найбільшого поширення набули лінійна і лінійно-штабна структура. Лінійна структура характеризується чітким підпорядкування єдиному начальнику, кожен співробітник підпорядкований тільки одній вищестоящій особі.

Лінійно-штабна структура являє собою лінійну структуру, доповнену штабним органом (штабом), на який покладаються додаткові функції управління . Така структура створюється зазвичай тоді, коли велика кількість співробітників або їх територіальна роз'єднаність не дозволяють начальнику служби безпеки ефективно управляти ними [49, с. 100].

Аналіз робіт різних авторів свідчить про те, що їхні погляди на кількість і назви структурних підрозділів служб безпеки не завжди збігаються.

Методи управління службою безпеки поділяються на три групи: економічні, організаційно-розпорядчі та соціально-психологічні [56, с. 143]. Керівники служби безпеки повинні бездоганно володіти всіма методами управління в їх єдності . Для цього вони повинні знати особливості кожного з них.

Так, на рівні співробітника служби безпеки переважним впливом користується такий економічний стимул, як заробітна плата. Вміле використання цього стимулу з урахуванням рівня професіоналізму, стажу роботи, результатів діяльності співробітника і т.д. дозволяє в значній мірі підвищити його трудову активність.

Організаційно-розпорядчі методи управління (накази, розпорядження, вказівки, інструкції тощо) поділяються на три групи: розпорядчі, організаційно - стабілізуючі та дисциплінуючі . Особливу увагу в діяльності

служби безпеки слід приділити таким нормативам, як нормативи часу виконання тієї чи іншої діяльності, чисельності співробітників того чи іншого підрозділу і т.д. Такі нормативи зазвичай переймають з досвіду роботи органів внутрішніх справ, з поправкою на специфіку діяльності служби безпеки підприємства.

Соціально- психологічні методи засновані на використанні моральних стимулів до праці і впливають на особистість співробітника служби безпеки за допомогою психологічних прийомів з метою перетворення в усвідомлений борг, внутрішню потребу людини. Це досягається за допомогою прийомів, які носять особистісний характер (особистий приклад, авторитет і т.д.). На рівні колективу служби безпеки діють методи, що включають оцінку індивідуальних якостей співробітників і вироблення орієнтирів, створюють умови для максимального прояву їх професійних якостей.

Принципи управління службою безпеки визначають вимоги до системи, структури та організації процесу управління . У рамках служби безпеки І. Нежданов виділяє такі принципи:

1 . Науковість.

2 . Єдиноначальність і колегіальність.

3 . Принцип системності та комплексності.

4 . Принцип оптимального поєднання централізації і децентралізації.

5 . Принцип плановості.

6 . Принцип поєднання прав, обов'язків і відповідальності [66].

Важливе місце в механізмі управління займають критерії ефективності управління діяльністю служби безпеки. Таким загальним критерієм, на наш погляд, може бути здатність керівництва служби безпеки при мінімальних ресурсах і за певний проміжок часу досягти поставленої мети у формі конкретних результатів.

Зрозуміло, цей критерій може бути зрозумілий тільки через систему кількісних показників, які розкривають його сутність. На практиці, зазвичай, застосовують такі показники, як кількість затриманих правопорушників,сума

(у гривнях) можливого збитку щодо запобігання та припинення злочинів і адміністративних правопорушеннях і т.д. Оскільки до теперішнього часу нормативно закріплених критеріїв ефективності діяльності служб безпеки немає, то за відсутності цієї базової основи дуже складно розробити критерії оцінки ефективності управління ними .

Структура процесу управління в узагальненому вигляді складається з трьох стадій, кожна з яких включає в себе послідовно здійснювані етапи або операції:

І стадія . Збір, обробка, узагальнення та аналіз інформації.

ІІ стадія . Вироблення і прийняття управлінського рішення .

ІІІ стадія . Організація виконання управлінського рішення [68, с. 12].

Зрозуміло, така структура процесу управління не є загальноприйнятною, яку слід копіювати при управлінні діяльністю служби безпеки.Виходячи зі специфіки діяльності самої служби безпеки та її зовнішнього оточення, слід (у рамках вищевказаної структури процесу управління) виробляти свій підхід до процесу управління .

Проблемою, яка найчастіше зустрічається у процесі управління службою безпеки підприємства є проблема нечіткого розмежування повноважень, що приводить не лише до дублювання функцій, а що значно гірше – до відсутності чіткого розуміння підпорядкування. Особливо така ситуація виникає тоді, коли засновниками підприємства є кілька осіб, і кожен з них має власне бачення загроз і можливих шляхів протидії останнім. Отож, якщо у статутних документах немає чіткого розмежування сфер, кожен із засновників за які відповідає, то і для діяльності служби безпеки це створює загрозу подвійного підпорядкування.

Таким чином, раціональне впровадження в практику основних елементів системи, механізму та процесу управління дозволить керівництву служби безпеки значно підвищити ефективність управлінського впливу на результати його діяльності.

2.3. **Національна та іноземна практика структурної організації служби безпеки підприємства та завдання, які вирішуються кожним із підрозділів**

В умовах загострення конкурентної боротьби і зростання злочинності роль і значення розвідки служби безпеки підприємства буде постійно підвищуватися. Такий висновок випливає не тільки з досвіду країн з розвинутою ринковою економікою, таких як США, Великобританія, Франція, але також з усвідомлення вітчизняними підприємцями практичної потреби отримання знань попереджувального характеру про тенденції, факти, явища і т.д., що існують поза підприємством . Інформацію такого роду здатна надавати (за належної організації її роботи) розвідувальний підрозділ служби безпеки. Перед цим підрозділом зазвичай ставиться одна мета: своєчасне виявлення і надання керівництву підприємства закритої інформації про реальні та потенційні зовнішні загрози для безпеки функціонування суб'єкта.

Звичайно, мету розвідувальної діяльності можна сформулювати й іншим чином, але в будь-якому випадку вона повинна відображати наступні моменти . По-перше, своєчасність виявлення та подання керівництву підприємства необхідної інформації (цілком очевидно, що відсутність або запізнювання відповідної інформації не дозволить вжити заходів щодо ліквідації або нейтралізації загроз діяльності підприємства).

По-друге, необхідно поставляти керівнику не будь-яку, а лише якісну та потрібну інформацію. Такою вона буде в тому випадку, якщо встановлені: а) важливість (здатність внести вклад в діяльність підприємства), б) точність (надійність джерела і самої інформації); в) значимість (цінність і правильне розуміння інформації) [80, с. 65]. Нарешті, по-третє, сфера дій розвідки повинна знаходитися у зовнішньому середовищі функціонування підприємства .

Саме зовнішнє середовище функціонування підприємства є об'єктом розвідувальної діяльності служби безпеки. Воно включає в себе:

1. Постачальників (юридичні та фізичні особи, які забезпечують підприємство та його конкурентів матеріальними ресурсами, необхідними для виробництва конкретних товарів або послуг).

2. Маркетингових посередників (фірми, що допомагають підприємству в просуванні, збуті і розповсюдженні його товарів серед клієнтів).

3. Клієнтів (окремих осіб, що купують товари і послуги для особистого споживання; організації, що купують товари і послуги для використання їх у процесі виробництва; організації, що купують товари і послуги для наступного перепродажу їх з прибутком для себе; державні організації, що купують товари і послуги або для подальшого їх використання у сфері комунальних послуг, або для передачі цих товарів і послуг тим, хто їх потребує; зарубіжні споживачі, виробники, проміжні продавці і державні установи) .

4 . Конкурентів .

5 . Контактні аудиторії (будь-яка група, яка проявляє реальний або потенційний інтерес до підприємства або впливає на його здатність досягати поставлених цілей), що включають в себе:фінансові кола (банки, інвестиційні компанії, брокерські фірми, фондові біржі, акціонери); засоби масової інформації (газети, журнали, радіостанції, телецентри і т.д.); державні установи, чия діяльність здатна негативно впливати на роботу підприємства;цивільні групи дій (організації споживачів, екологічні об'єднання, групи, що представляють національні меншини і т.д.); місцеві контактні аудиторії (організації самоврядування, злочинні угруповання, первинні осередки громадських рухів і партій і т.д.).

Досягнення мети, поставленої перед розвідкою, можливо при реалізації наступних завдань:

• виявлення правопорушень, які зачіпають економічні інтереси підприємства;

• своєчасне інформування про методи, способи і осіб, що мають намір завдати шкоди підприємству та / або його персоналу;

• сприяння правоохоронним, судовим і контрольно-наглядовим органам у притягненні до відповідальності юридичних і фізичних осіб, дії яких зачіпають інтереси підприємства-засновника.

Викладені нами вище міркування про цілі, завдання і функції розвідувального підрозділу служби безпеки, якщо вони будуть прийняті на практиці, вирішальною мірою визначають його структуру .

Загальноприйнятим вважається твердження про те, що потенціал розвідки безпосередньо залежить від наявності та якості відповідних сил і засобів.

Серед найважливіших засобів розвідувальної діяльності - розвідувальна техніка. До неї належать:

• засоби проникнення (відмички, піроленти, різаки, спеціальні засоби);

• підслуховуючі пристрої (мікрофони, електронні стетоскопи, системи прослуховування телефонів, факсів тощо);

• системи прихованого відеоспостереження (мініатюрні камери, пристрої з об'єктивом «вушко голки», ендоскопи, теле-, фотоапаратура стеження);

• системи комп'ютерного шпигунства (система перехоплення комп'ютерної інформації).

Нагадаємо, що за нормами національного законодавства не передбачене використання засобів спецтехніки іншими особами, аніж представниками правоохоронних органів. До того ж, якщо навіть використовуючи приховану техніку представники служби безпеки підприємства зафіксують факти, що мають визначальне значення для розгляду справи про порушення прав та інтересів підприємства, такий матеріал все ж буде визнано неналежним доказом у суді. Тобто, станом на сьогоднішній день використання спецтехніки службою безпеки підприємства знаходиться поза межами закону.

У розвідувальній діяльності служб безпеки підприємств іноземних держав застосовуються переважно такі методи:

• приховане спостереження за людьми і стаціонарними об'єктами;

• зашифроване опитування осіб, які можуть надати цінну інформацію;

• вивчення предметів і документів закритого характеру;

• конфіденційне наведення довідок;

• зашифрований зовнішній огляд споруд, приміщень та інших об'єктів [48].

Зрозуміло, не забороняється вивчення відкритих джерел інформації (газет, журналів, бюлетенів тощо), гласний зовнішній огляд об'єктів. Однак використання цих методів у розвідці практикується тільки в якості додаткових і другорядних методів. У кожному разі відкриті джерела інформації перепровіряються розвідувальними методами.

Наприклад, аналізуючи транспортну документацію (коносамент, договір залізничного перевезення і т.д.), можна отримати уявлення про кількісні, а іноді і цінові параметри товарообігу фірми, щодосліджується . Однак, щоб це подання перейшло в точні знання, необхідно отримати від інформаторів, які висвітлюють діяльність цієї фірми, ряд інших відомостей. Взаємодоповнюючі один одного відомості інформаторів і аналіз основних документів дозволять дати точну і об'єктивну оцінку що відбувається в цій фірмі . Без застосування негласних методів отримати таку оцінку практично неможливо. Цей приклад підтверджує правило, якому повинна слідувати будь-яка розвідка: інформація, отримана з використанням легальних можливостей, повинна обов'язково перевіряти ще за допомогою негласних інформаторів.

Основні методи отримання розвідувальної інформації можна представити у наступному вигляді:

Таблиця 2.1.

Основні методи отримання розвідувальних відомостей [88]

Людина	Спосіб вивчення	Виріб (процес)
1. Допит працівників конкуруючої фірми	1. Вивчення судових документів	1. Фотографування моделей, експонатів тощо на виставках і конференціях
2. Допит працівників свого підприємства	2. Збирання і аналіз відомостей, що містяться в засобах масової інформації	2. Кіно-, фото - й відеоматеріали
3. Замасковані навички "виманювання" необхідної інформації на конференціях, семінарах, симпозіумах та ін.	3. Вивчення фінансових документів конкурентів	3. Комп'ютерні програми
4. Проведення "помилкових" переговорів з фахівцями конкуруючої фірми	4. Збирання й вивчення проспектів, брошур, які видають конкуренти	4. Аналіз відходів виробництва
5. Наймання на роботу службовця конкуруючої фірми для отримання відомостей, що становлять комерційну таємницю	5. Аналіз відомостей, що містяться у відомчих виданнях	5. Купівля товару конкурента у третіх осіб
6."Неправдиві*' переговори з фірмою-конкурентом щодо придбання ліцензії	6. Збирання копій документів правоохоронних і контрольно-наглядових органів (преси)	
7. Створення фіктивних підприємств, які пропонують роботу фахівцям із конкуруючих фірм	7. Копіювання документів	
8. Негласне ознайомлення	8. Використання загублених документів	
9. Підслуховування розмов, які відкрито (не таючись) ведуть між собою співбесідники	9. Використання звітів (копій) з перевірок на поліграфі ("детекторі брехні"^	
10. Бесіда із працівниками правоохоронних і контрольно-наглядових органів		

Цілком очевидно, що наведені методи не можуть бути вичерпними. Найбільш важливим джерелом розвідувальних відомостей в тріаді «людина - документ - виріб (процес) » є, безумовно, людина .

Так, отримання будь-якої інформації можливе у особи, здатної за різними мотивами видати важливу інформацію. Проте по-справжньому цінну інформацію можна отримати тільки від залучених до співпраці інформаторів.

Інформаторів розвідувального підрозділу можна умовно розділити на кілька груп:

1 . Співробітники свого підприємства, що контактують в силу свого службового становища із зовнішніми джерелами інформації.

2 . Персонал інших підприємств, установ і організацій, що мають доступ до циркулюючої всередині них закритої службової інформації.

3 . Особи вільних професій або непрацюючі,що мають контакти з співробітниками інших підприємств, громадських організацій, партій, громадських рухів і з представниками неформальних структур.

4 . Співробітники розвідувального підрозділу служби безпеки,що працюють під прикриттям на інших підприємствах чи в неформальних групах і т.д.

Слід особливо підкреслити, що вищевказані інформатори (крім співробітників розвідки) не обов'язково повинні чітко усвідомлювати свою роль і свідомо співпрацювати з співробітниками розвідувального підрозділу .

Найціннішим джерелом розвідувальної інформації після людини є документ. Іноді неможливо роздобути оригінал будь-якого документа, тому вдаються до отримання його копії, а як її придбати, розвідник повинен знати.

Щоб добути той чи інший документ для зняття з нього копії, необхідно попередньо скласти документограму (графічне зображення руху, динаміки документаційних процесів, що протікають на підприємстві від створення документа до моменту здачі його в архів). Це дозволить виявити ті вузлові точки, в яких можливе в принципі «зняття» необхідної інформації.

Кінцевий продукт розвідувальної діяльності - інформація та докази.

Інформаційна робота - це процес, в результаті якого сирі факти перетворюються в закінчену продукцію розвідувальної діяльності [92, с.

335].Вся зібрана розвідувальна інформація на підставі її кінцевого використання класифікується за такими категоріями:

1 . сигнальна (або що попереджає);

2 . тактична (тобто інформація, яка вимагає негайних дій);

3 . стратегічна (тобто інформація, яка збирається протягом відносно довгого часу і аналізується);

4 . доказова (тобто дані у формі документів і предметів, що подаються до правоохоронних, судових та контрольно-наглядові органи) [93, с. 441].

Вся зібрана і оброблена інформація представляється керівництву підприємства у формі розвідувального огляду, довідки-меморандуму, повідомлення і т.д. Незважаючи на різноманітність цих документів, їх інформація повинна містити: а) виклад фактичних даних, б) джерела інформації (щодо інформаторів без їх розшифровки), в) висновки; г) пропозиції .

Надійність джерела і достовірність інформації оцінюється керівництвом розвідки за допомогою цифрових і буквених шифрів.

Збирання доказів включає в себе наступні елементи:1) пошук і виявлення доказів; 2) фіксацію виявленого в документах; 3) вилучення доказів.

Документування розвідувальної інформації здійснюється за трьома основними напрямками: встановлення осіб, які можуть бути свідками у кримінальній або цивільній справі, виявлення предметів, що можуть бути джерелами доказів; пояснення, висновки експертів, письмові і речові докази; фіксація дій правопорушників .

Об'єктивну комплексну оцінку результатів роботи розвідки можуть дати тільки керівники підприємства-засновника.

Критеріями роботи розвідувального підрозділу можуть бути:

1 . точність і об'єктивність відомостей про досліджуваних особах;

2 . якісне документування протиправних дій юридичних та фізичних осіб, спрямованих проти інтересів підприємства-засновника;

3 . своєчасне і об'єктивне інформування про зовнішні реальні та потенційні загрози і їх носії.

Окрім розвідувальної діяльності у структурі служби безпеки підприємства обов’язково має бути присутній і контр розвідувальний підрозділ.

Значення і роль контррозвідки служби безпеки підприємства в сучасних умовах життя обумовлено принаймні двома обставинами: по-перше, прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів за допомогою засобів економічного шпигунства, по-друге, розширенням масштабу криміналізації населення, що створює поживний грунт для його певних верств вирішувати свої потреби злочинним шляхом. Виходячи з цього, мету контррозвідувального підрозділу можна визначити як протидія розвідувальним заходам конкурентів і припинення правопорушень з боку протиправних груп або окремих осіб, які посягають на інтереси підприємства або його окремих співробітників.

Про призначення контррозвідки точно і стисло висловився А. Г. Шаваєв: «Контррозвідка займається в основному захистом і оборонної діяльністю» [94]. На відміну від розвідки, об'єктом контррозвідувальної діяльності є не зовнішнє, а внутрішнє середовище функціонування підприємства. Це середовище включає в себе, принаймні, такі елементи:

1 . Керівний склад підприємства (директор, його заступники, головний бухгалтер і т.д.) як потенційні об'єкти розвідувальних заходів та / або злочинів з боку конкурентів.

2 . Особи з допоміжного персоналу, які мають доступ до комерційної таємниці (оператори, працівники канцелярії і т.д.).

3 . Співробітники, з боку яких потенційно існує небезпека надання злочинним елементам таких відомостей, які допоможуть їм здійснити злочин (сторожі, охоронці, водії керівників і т.д.).

4 . Співробітники самої служби безпеки .

5 . Раніше судимі особи з числа працівників підприємства .

6 . Співробітники підприємства, родичі яких працюють у конкурентів.

7 . Раніше звільнені з підприємства його працівники .

8 . Особи, які в силу своїх посадових обов'язків регулярно приймають відвідувачів підприємства .

Визначення мети та об'єкта контррозвідувальної діяльності дозволяє визначити коло можливих завдань підрозділу контррозвідки:

• боротьба з економічним шпигунством;

• припинення злочинів проти окремих груп співробітників (або всіх співробітників на їх робочих місцях);

• надання сприяння правоохоронним, судовим і контрольно- наглядовим органам в документуванні протиправних дій осіб, які вчиняють кримінальні злочини і адміністративні проступки [92, с. 336].

Виконання вищевказаних завдань можливе при реалізації наступної сукупності функцій контррозвідки:

• збір відомостей і документів у цивільних і кримінальних справах;

• регулярне інформування керівництва підприємства про причини, що породжують і умовах, що сприяють вчиненню правопорушень з боку персоналу;

• документування дій осіб, затриманих за адміністративні проступки;

• виявлення осіб з числа персоналу, які сприяють злочинним елементам (які не працюють на підприємстві) у вчиненні ними злочинів;

• викриття економічних (промислових) шпигунів з числа персоналу;

• інформування керівників підприємства і охоронців (якщо вони є) про плановані щодо їх злочини;

• пошук безвісти зниклих співробітників підприємства;

• створення умов, що виключають підслуховування розмов у службових кабінетах;

• встановлення обставин розголошення відомостей, що становлять комерційну таємницю;

• з'ясування біографічних та інших, що характеризують особу даних про співробітників підприємства (з їхньої письмової згоди) при укладенні ними трудових контрактів;

• пошук втраченого співробітниками майна, що належить підприємству;

• консультування персоналу з питань забезпечення безпеки підприємства [88].

На основі затверджених керівництвом служби безпеки і підприємства цілей, завдань і функцій контррозвідки можливе формування її оргструктури. У структурі контррозвідки, на наш погляд, повинні функціонувати такі підрозділи: власної безпеки, проведення розслідувань, по роботі з інформаторами, довідково -інформаційний фонд (ДІФ), попередження правопорушень, з технічного забезпечення проведення операцій, з організації збереження комерційної таємниці, негласного проникнення, організації дезинформаційних заходів, комп'ютерної безпеки.

Підрозділи (відділення, групи, сектори) контррозвідки умовно можна розділити на дві групи:

• а) основні, які власне і вирішують завдання, поставлені перед контррозвідкою (проведення розслідувань, робота з інформаторами і т.д.);

• б) допоміжні, основними завданнями яких є всебічне сприяння співробітникам основної групи (ДІФ, технічне забезпечення проведення операцій і т.д.).

Схематично розмежування діяльності структурних підрозділів контррозвідки можна представити наступним чином:

Таблиця 2.2.

Розмежування діяльності структурних підрозділів контррозвідки

Назва підрозділу	**Завдання**	**Форма подання результатів роботи**
1. Відділення (група, сектор) власної безпеки	Документування протиправних і аморальних дій працівників служби безпеки	Рапорт, довідка, протокол спостереження, огляди

2. Відділення (група, сектор) проведення розслідувань	Збирання і аналіз інформації про правопорушення і надзвичайні ситуації	Рапорт, аналітична довідка, справа (досьє)
3. відділення (група, сектор) роботи 3 інформаторами	Залучення до співпраці інформаторів і отримання від них регулярної інформації про перебування на об'єкті, що охороняється, і серед його персоналу	Справа (досьє), аналітичні огляди, довідка щодо кожного повідомлення інформатора
4. Довідково-інформаційний фонд	Ведення звітів, зберігання і видача співробітникам необхідної інформації (досьє) тощо	Довідки, аналітичні огляди, облікові картки, меморандуми
5. Відділення (група, сектор) із запобігання правопорушенням	Аналіз правопорядку на підприємстві і пропозиції керівництву підприємства про усунення причин та умов, виникнення правопорушень на об'єкті, що охороняється	Досьє (справа), аналітичні довідки
6. Відділення (група, сектор) з технічного забезпечення проведення операцій	Установлення та експлуатація технічних засобів, їх надання співробітникам інших груп	Акти, кіно -, фотокадри, звукозапис т. ін.
7. Відділення (група, сектор) організації збереження комерційної таємниці	Створення технічних умов, що запобігають витоку комерційної таємниці	Акти перевірок, протоколи обстеження приміщень, інструкції для персоналу підприємства тощо
8. Відділення (група, сектор) негласного проникнення	Висвітлення стану правопорядку і трудової дисципліни в колективі підприємства	Рапорти, огляди, аналітичні записки
9. Відділення (група, сектор) організації дезінформаційних заходів	Організація заходів, що вводять в оману конкурентів і злочинців	Плани дезінформаційних заходів, звіти, довідки
10. Відділення (група, сектор) комп'ютерної безпеки	Захист комп'ютерних мереж від несанкціонованого доступу до них	Звіти, довідки

Кількісне співвідношення між співробітниками допоміжних і основних відділень (груп, секторів) контррозвідки може бути різним, однак при цьому дві умови повинні бути дотримані обов'язково: співробітники допоміжних підрозділів надають допомогу співробітникам основних підрозділів (а не навпаки); робота співробітників основних підрозділів повинна бути ефективною.

Відомо, що комплекс сил, засобів контррозвідки і застосовуваних нею методів у величезній мірі визначає потенціал контррозвідувальної діяльності. Правда, умовою реалізації цього потенціалу є активна організаційно - управлінська діяльність керівництва СБ, проте своєрідним базисом такої діяльності є таки вищезгаданий комплекс сил, засобів і методів.

Серед засобів контррозвідувальної діяльності найбільшу увагу слід приділити фінансовим . Направляти їх слід (крім оплати праці детективів і технічного їх забезпечення), в першу чергу, на заохочення праці інформаторів, проведення операцій, транспортні витрати і т.д.

Серед правових засобів до числа обов'язкових, без чого неможливе існування в принципі підрозділу контррозвідки, слід віднести положення про сектор (групу) контррозвідки, посадові інструкції і положення про режим. До матеріально-технічних засобів відносять зазвичай автомобілі, телефони,фотоапарати, диктофони і т.д. Відносно технічних засобів слід мати на увазі, що їх використання обмежене законодавчими нормами.

Інформаційні засоби займають, з деякими застереженнями, центральне місце в системі засобів контррозвідки. Такий стан є закономірним, якщо мати на увазі, що продуктом контррозвідувальної діяльності є знання про цікавить об'єкті, причому не всякі, а нові знання. До числа інформаційних засобів відносяться різні обліки, що допомагають детективам контррозвідки в їх роботі (причому не завжди доцільно вводити їх в комп'ютерні системи).

Для об'єктивної оцінки діяльності контррозвідки необхідно розробити відповідні критерії та показники її діяльності. Критерії діяльності контррозвідувального підрозділу: а) ступінь протидії розвідувальним заходам

ділових конкурентів і злочинців, б) рівень запобігання і припинення правопорушень на об'єкті, що охороняється . Показниками, що розкривають вищевказані критерії, можуть бути:

1 . кількість притягнутих до відповідальності за розголошення комерційної таємниці підприємства;

2 . кількість виявлених економічних (промислових) шпигунів;

3 . кількість реалізованих інформаційних матеріалів про причини, що породжують і умов, що сприяють вчиненню правопорушень;

4 . кількість виграних судових процесів у цивільних справах на підставі матеріалів контррозвідки;

5 . кількість виграних судових процесів у кримінальних справах на підставі матеріалів контррозвідки;

6 . кількість розглянутих матеріалів, підготовлених контррозвідкою, з адміністративних правопорушень;

7 . кількість службових розслідувань, що проводяться відносно персоналу підприємства;

8 . кількість розшуканих безвісти зниклих співробітників підприємства;

9 . кількість перевірок співробітників підприємства;

10 . кількість повернутого підприємству втраченого його співробітниками майна .

Створення розвідувального, контррозвідувального і охоронного підрозділів у службі безпеки є обов'язковою умовою її існування. Штабний підрозділ створюється в разі, якщо вищевказані підрозділи є великими (за кількістю їхніх співробітників) і складними (за кількістю їх функцій) структурними формуваннями .

Наявність штабного підрозділу свідчить про високий рівень організаційної структури. Організація роботи штабу спрямована на створення необхідних умов для виконання його працівниками службових завдань і включає в себе:

• розподіл і закріплення в посадових інструкціях обов'язків, прав і відповідальності співробітників;

• визначення розпорядку дня та режиму роботи співробітників;

• забезпечення співробітників штабу інформаційно-аналітичними матеріалами (планами і графіками роботи, звітами, протоколами нарад і заслуховувань, правовими актами, матеріалами листування, методичними документами, публікаціями та ін);

• планування своєї діяльності;

• організацію виконання рішень (визначення виконавців, термінів, проведення інструктажів, нарад і т.д.);

• організацію контролю, обліку та оцінки діяльності;

• порядок здійснення взаємодії всередині штабу (визначення форм і процедур взаємодії, порядку обміну інформацією, підведення підсумків спільної роботи тощо);

• забезпечення матеріально-технічними засобами та їх експлуатацію (комп'ютерної та іншої оргтехнікою, витратними матеріалами, засобами зв'язку, іншим обладнанням, своєчасне їх обслуговування та ремонт);

• ефективне застосування матеріальних і моральних стимулів щодо співробітників штабу [85, с. 102].

Основними принципами, якими повинна бути пронизана вся робота штабу, є: організованість, цілеспрямованість, оперативність, передбачення і передбачливість, точність і ретельність, ініціатива і творчість.

Основна мета діяльності штабного підрозділу полягає в забезпеченні найбільш ефективного функціонування основних підрозділів (розвідки, контррозвідки та охорони) і всієї системи служби безпеки в цілому. Досягнення цієї мети можливе на основі реалізації наступних завдань: комплексний аналіз у сфері правопорядку; інтеграція діяльності підрозділів по досягненню загальних завдань, поставлених перед службою безпеки; надання ефективної допомоги підлеглим підрозділам; своєчасне подання на затвердження начальника служби безпеки проектів управлінських рішень .

Досягнення вищезазначених цілей і завдань можливе за умови реалізації наступних функцій:

• прийняття та реалізація найбільш кваліфікованих рішень у критичних ситуаціях;

• ресурсне забезпечення діяльності служби безпеки;

• планування діяльності служби безпеки;

• організація контролю виконання заходів;

• комплексне інспектування підпорядкованих підрозділів;

• організація взаємодії та координації між підрозділами;

• забезпечення інформацією співробітників підрозділів і керівників підприємства;

• організація зв'язку з громадськістю;

• правове забезпечення діяльності служби безпеки;

• вивчення, узагальнення та поширення позитивного досвіду діяльності підрозділів;

• організаційно-штатне забезпечення служби безпеки;

• організація ефективного використання зв'язку .

Практика доводить, що у складі штабу доцільно створити такі підрозділи: аналізу і планування, зв'язків з громадськістю, ресурсного забезпечення, чергової частини, довідково-інформаційного фонду, кабінету передового досвіду, організаційно - інспекторського, юридичної та криптографічного захисту.

Критерієм ефективної діяльності штабного підрозділу можна визнати якість його управлінського впливу на підрозділи служби безпеки в цілому і його підрозділів окремо. Показниками, що розкривають цей критерій, є: ступінь досягнення мети планів; своєчасне і повне забезпечення ресурсами підрозділів служби безпеки за встановленими нормами; оперативне та якісне виявлення недоліків і позитивного передового досвіду, виявленого в процесі контролю і комплексного інспектування; достатнє і своєчасне надання

співробітникам служби безпеки встановлених видів інформаційних документів .

Аналіз практики функціонування служб безпеки дозволяє стверджувати, що слабка ефективність їх діяльності в значній мірі є наслідком існування різних проблем. Всі ці проблеми настільки переплетені одна з одною, що розмежування їх між собою на практиці неможливо. Серед основних проблем національних служб безпеки підприємств можна назвати неефективну взаємодію служб безпеки з правоохоронними органами; заборона на носіння та застосування зброї; відсутність належно закріпленого в законодавстві правового статусу служби безпеки; відсутність у керівників служб безпеки необхідних правових та організаційно-управлінських знань, умінь і навичок тощо.

Цілком очевидно, що нами перерахована тільки частина проблем діяльності служб безпеки підприємств . Однак сама їх постановка дозволяє стверджувати, що рано чи пізно вирішувати їх доведеться.

Висновок до розділу 2.

Дослідження практики організації та управління службою безпеки підприємства дозволило сформувати нам наступні висновки:

1. Для створення служби безпеки на підприємстві необхідне здійснення комплексу організаційних та правових заходів. До організаційних заходів слід віднести: визначення структури служби безпеки та необхідної кількості працівників у кожному із підрозділів; проведення кадрового відбору працівників та керівника служби, надання необхідного інформаційного, матеріально-технічного та усіх інших видів забезпечення. До правових заходів належать: включення положень про службу безпеки підприємства до Статуту, розроблення відповідних положень на наказів про службу безпеки та усі її підрозділи, опрацювання та прийняття посадових інструкцій для працівників служби.

2. Проведення науково-практичного аналізу принципів та етапів управління службою безпеки підприємства дозволило нам дійти до висновку, що основною проблемою управління є нечітке розмежування функцій управління між засновниками підприємства. Для вирішення вказаної проблеми доцільним було б нормативно визначити таке розмежування у статутних документах суб'єкта господарювання.

3. Аналіз іноземної практики структурної організації служби безпеки підприємств дозволив нам встановити, що найчастіше служба складається із чотирьох підрозділів: розвідувального, контррозвідувального, штрабного та охоронного. Кожен із підрозділів може містити свою структуру, величину і чисельність якої визначають в залежності від завдань, які стоять перед службою безпеки підприємств. Часто на практиці зустрічаються випадки об'єднання розвідувального та контррозвідувального підрозділів у один, проте це вимушена дія через брак матеріальних ресурсів. Штабні підрозділи присутні на тих підприємствах, які володіють достатньо великою чисельно структурою служби безпеки і при цьому керівник служби не в змозі від слідкувати усі напрямки роботи служби. Тобто, штабні підрозділи присутні фактично лише на великих підприємствах, які до того ж мають значну кількість відокремлених структурних підрозділів. Охоронні підрозділи є обов'язковими у структурі служб безпеки підприємств, а їх чисельність в основному залежить від величини ресурсів підприємства, які необхідно охороняти.

Національна практика структурної побудови служб безпеки намагається копіювати іноземну, проте відсутність норм законів щодо визначення основоположних засад діяльності відповідних служб впливає на те, що діяльність по розвідувальній та контр розвідувальній діяльності перебуває за межами закону.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ПОКРАЩЕННЯ ДІЯЛЬНОСТІ СЛУЖБ БЕЗПЕКИ ПІДПРИЄМВА

Поняття конкурентної розвідки, яка здійснюється службою безпеки підприємства включає безліч аспектів, не лише дії по збору інформації про конкурентів, але і методи вивчення зібраної інформації, організації роботи, розроблення заходів для захисту інтересів фірми від дій конкурентів.

І тут необхідно відзначити, що один з найбільш ефективних інструментів конкурентної розвідки з метою підвищення конкурентоспроможності своїх товарів на ринку є застосування бенчмаркінгу.

Термін "бенчмаркінг" вперше в бізнесі був застосований у 1972 р. в ході досліджень, проведених Інститутом стратегічного планування в Кембріджі (США), що були спрямовані на пошук ефективних рішень у сфері конкуренції [88].

Так, американська авіакомпанія Southwest Airlines вирішила поліпшити свої фінансові показники. Опитавши клієнтів, менеджери зрозуміли, що завоювати їх симпатії можна більш зручним розкладом і збільшенням числа рейсів. Залишилося придумати, як вичавити з наявного авіапарку по максимуму. Для початку менеджери розрахували, скільки часу йде на заправку літака, технічне обслуговування та інше. І дійшли висновку: необхідно скоротити час перебування літака на землі, не порушуючи при цьому технічних норм . Але як це зробити? Звернувшись до досвіду інших авіапідприємств, компанія виявила, що за часом обслуговування літаків вона і зараз поза конкуренцією. Хтось із службовців звернув увагу на те, що еталоном швидкості обслуговування транспортного засобу вважаються автогонки. Менеджери авіакомпанії вивчили спеціальну літературу і познайомилися з основними принципами командної роботи техніків. А потім впровадили ці ж принципи у себе. Звичайно, авіакомпанія не змогла обслуговувати літаки з такою ж швидкістю, з якою у "Формулі- 1" обслуговують машини , однак час на цю процедуру скоротилося з 45 до 15

хвилин, а кількість рейсів збільшилася. Ця історія - типовий приклад використання маркетингового інструменту під назвою "бенчмаркінг" . З його допомогою компанії можуть підвищити свою конкурентоспроможність.

Як одна з найважливіших функцій маркетингової діяльності, бенчмаркінг являє собою: а) безупинний процес дослідження технологій, процесів, методів організації виробництва і збуту продукції, менеджменту в кращих компаніях партнерів і конкурентів з метою підвищення ефективності власної фірми;б) науковий метод аналізу переваг й оцінювання конкурентних переваг партнерів і конкурентів однотипної чи суміжної галузі з метою вивчення і використання всього кращого у власній фірмі; в) мистецтво виявляти і використовувати у своєму бізнесі те, що інші роблять краще, тобто реалізовувати на практиці принцип "від кращого до найкращого".

Бенчмаркінг, будучи одним з найважливіших напрямків стратегічно орієнтованих маркетингових досліджень, характеризується можливостями, що представлені у таблиці 3.1.

Таблиця 3.1.

Можливості бенчмаркінгу [24]

Харатеристики процесу дослідження	**Значення бенчмаркінку в стратегічно орієнтованих маркетингових дослідженнях**	
	Дослідження ринку	**Аналіз конкурентів**
Загальна мета	Аналіз ринку, ринкових сегментів чи визначення товарів	Аналіз стратегій конкурентів
Предмет вивчення	Потреби покупців	Стратегії конкурентів
Об’єкт вивчення	Товари і послуги	Ринки і товари
Основні обмеження	Ступінь задоволеності покупців	Діяльність на ринку
Значення для ухвалення рішення	Незначне	Деяке
Основні джерела інформації	Покупці	Галузеві експерти і аналітики

До основних принципів концепції бенчмаркінгу відносяться:

- концентрація на якості;

- важливість бізнес-процесів - бізнес-процеси, що протікають у компанії, набагато важливіші, ніж процеси функціонування класичних підрозділів;

- систематичне проведення загального бенчмаркінгу - безупинне, всебічне і ретельне вивчення як основних конкурентів компанії, так і кращих прикладів і зразків світової практики;

- плановість у роботі;

- вимірність характеристик і їхня вірогідність - бенчмаркінг вимагає порівняння ключових характеристик критичних процесів, обмірюваних у декількох компаніях;

- цілями бенчмаркінгу є: визначення конкурентоспроможності компанії, її слабких сторін; усвідомлення необхідності змін; добір ідей по кардинальному поліпшенню бізнес-процесів; виявлення найкращих прийомів роботи для компаній даного типу; розробка інноваційних підходів до удосконалювання бізнес - процесів;

- сприяння установленню перспективних цільових показників якості роботи, що значно перевершує поточні; розробка нових прийомів підвищення якості наданих послуг і ефективності роботи;

- переорієнтація корпоративної культури і ментальності.

До основних видів бенчмаркінгу відносяться:

а) внутрішній - зіставлення характеру і якості роботи аналогічних підрозділів у межах компанії;

б) конкурентоспроможності - порівняння якості роботи даної компанії з її конкурентами на ринку;

в) функціональний - порівняння характеристик визначених функцій, виконуваних у різних компаніях аналогічного профілю;

г) загальний - найбільш складний вид, що дозволяє порівнювати бізнес - процеси, що протікають у компаніях, які відносяться до різних галузей промисловості [24].

Реалізація бенчмаркінгу здійснюється в кілька етапів:

1. визначення об'єкта, тобто функцій і процесів, що вимагають поліпшення в діяльності компанії. З цією метою необхідно вирішити ряд задач: вибрати критичні процеси, провести їхній ретельний аналіз і дати докладний опис;

2. визначити критичні фактори (індикатори) успіху функціонування на ринку, виділити процеси, зв'язані з реалізацією критичних факторів успіху, установити, чи не існує невідповідності між метою проведення бенчмаркінгу й основними цілями компанії, визначитися з джерелами інформації і методами її одержання. Іншими словами, на даному етапі необхідно знайти відповіді на питання: Чого компанія хоче досягти? Яким потенціалом вона володіє зараз? Що необхідно робити, щоб добратися до поставленої мети?

3. проведення внутрішнього обстеження, а саме вимір показників власної компанії. Для цього здійснюється збір, аналіз і узагальнення системи показників (ключових факторів успіху, індикаторів і ін. необхідних характеристик процесів, що поліпшуються, чи функцій);

4. ідентифікація кандидатів у партнери по бенчмаркінгу;

5. спостереження, збір інформації і вимірювання показників, які цікавлять, у діяльності партнерів по бенчмаркінгу.

6. аналіз отриманих результатів і їхня адаптація до діяльності компанії. Тут важливо усвідомити отримані результати щодо подібності і розходження в характеристиках, з'ясувати їхній взаємозв'язок; узагальнити й інтерпретувати отримані дані; виявити і проаналізувати "дельти" між критичними процесами й аналогічними процесами компанії - партнера; спрогнозувати "поводження дельти";

7. власне впровадження результатів бенчмаркінгу - остаточний вибір тих елементів процесів, що містять елементи безупинного удосконалювання;

8. з огляду на обмеженість інформаційного простору українського ринку, найбільшу складність у процесі бенчмаркінгу являє реалізація таких етапів, як ідентифікація кандидатів у партнери по бенчмаркінгу і спостереження, збір інформації і вимір показників, які цікавлять, у діяльності партнерів,

відібраних по бенчмаркінгу. Саме для вирішення означеної проблеми інформаційні послуги можуть надати спеціалізовані компанії, що мають доступ до різних джерел, включаючи міжнародні бази даних.

Перш ніж застосовуватибенчмаркінгяк інструментщодо вдосконалення діяльностіпідприємство повинновирішити, який обсягресурсіввономоже на ньоговиділити. Якщоприймаєтьсярішення використовуватибенчмаркінгв якостіодногоз інструментівпостійного вдосконалення, то він можебути виділенийвокремий процес діяльності служби безпеки підприємства.

У тому випадку, коли бенчмаркінг проведений правильно, він може дати компанії багато переваг. Критеріями успішного проведення бенчмаркінгу є правильно підібрана команда , глибока деталізація процесів , зацікавленість керівництва в результатах, інтеграція результатів бенчмаркінгу зі стратегічними планами розвитку .

Під час виконання робіт команда бенчмаркінгу має можливість подивитися на свою організацію з боку. Це дозволяє вийти за рамки щоденної діяльності та існуючих обмежень, і знайти нові ідеї щодо поліпшення роботи . Завдяки застосуванню бенчмаркінгу можна уникнути багатьох помилок, а також підвищити прибуток організації за відносно короткий час.

Чому ми розглядаємо бенчмаркінг як передумову до вдосконалення системи безпеки підприємства, що здійснюється силами служби безпеки суб’єкта господарювання? Та тому, що бенчмаркінг є сучасною та невід’ємною складовою ділової розвідки. Дехто із дослідників навіть порівнюють бенчмаркінг із промисловим шпіонажем, та між ними все-таки є суттєва, на нашу думку, різниця. І полягає вона у тому, що бенчмаркінг вивчає досвід конкурентів, який не закритий сімома замками, тоді як промисловий шпіонаж націлений на вивідування промислових секретів та іншої таємної інформації, викриття якої неминуче завдасть шкоди підприємству-власнику.

Реалізація основних операцій бенчмаркінгу повинна здійснюватися на основі певних принципів поведінки , яким повинна відповідати компанія, що проводить бенчмаркінг. У зв'язку з активним проведенням на території України євро інтеграційних процесів, для вироблення рекомендацій щодо застосуваннядосліджуваного методу вважаємо за доцільне спиратися на Європейський кодекс поведінки при бенчмаркінгу.

Вказаний кодекс встановлює основні принципи поведінки при бенчмаркінгу.

Принцип підготовки. Передбачає ретельну підготовку підприємства до процесу бенчмаркінгу на основі розробки анкет і графіка візитів на підприємство партнера з бенчмаркінгу, забезпечення юридичного супроводу процесу бенчмаркінгу .

Принцип контакту. Передбачає повагу корпоративної культури партнера з бенчмаркінгу, узгодження способу передачі інформації та отримання дозволу фізичних осіб на згадування їх прізвищ та координат як в контактний запитах, так і у відкритих дискусіях.

Принцип взаємообміну. Передбачає можливість взаємообміну інформацією з партнером по бенчмаркінгу при дотриманні умов законності і чесності.

Принцип конфіденційності. Розглядає відомості, отримані при бенчмаркінгу, як конфіденційні , які не можуть бути передані третім особам без попередньої згоди партнера з бенчмаркінгу . Крім того, участь самої організації - партнера в процесі бенчмаркінгу є конфіденційною .

Принцип використання. Припускає, що інформація, отримана за допомогою бенчмаркінгу , буде використана тільки в цілях , узгоджених з партнером по бенчмаркінгу . Використання в інформації імені партнера по бенчмаркінгу, отриманих відомостей або аналізованої діяльності вимагає попереднього дозволу цього партнера.

Принцип легальності . Припускає використання тільки законних методів отримання інформації.

Принцип завершеності. Передбачає своєчасне виконання кожного зобов'язання , заявленого з бенчмаркінгу .

Принцип розуміння і згоди. Передбачає узгодження з партнером по бенчмаркінгу напрямів використання наданої інформації.

Принцип взаємин з конкурентами . Передбачає встановлення додаткових принципів , що відносяться до обох партнерів по бенчмаркінгу у відносинах з реальними і потенційними конкурентами. Серед цих принципів: необхідність дотримання законодавства про конкуренцію, збереження комерційної таємниці, чітке узгодження обсягу, методів збору даних.

Європейський кодекс поведінки при бенчмаркінгу є рекомендаційним документом, основних принципів якого дотримуються процвітаючі європейські компанії, що проводять бенчмаркінгові дослідження .

Застосування національними підприємствами вищевикладених принципів і методів бенчмаркінгу сприятиме забезпеченню кращого взаєморозуміння українських та зарубіжних компаній, а це дозволить використовувати прогресивний зарубіжний досвід для вдосконалення виробництва вітчизняних підприємств.

Отож, як висновок можна стверджувати, що бенчмаркінг є одним із найефективніших способів дослідження ринку і його компонентів, втілення результатів якого сприяє підвищенню конкурентоспроможності товарів підприємства. Вказаний метод є легальним і не порушує жодних правил чесної конкуренції, а тому у час законодавчої невизначеності може стати хорошою основою для діяльності служби безпеки підприємства на шляху до забезпечення його економічної безпеки.

Висновок до розділу 3.

Дослідження перспектив покращення діяльності служб безпеки підприємств здійснювалось нами через аналіз новітнього процесу ділової розвідки – бенчмаркінгу.

В ході наукового аналізу літературних джерел із означеного питання нам вдалось встановити, що бенчмаркінг побудований на легальному і відкритому аналізу інформації про діяльність суб'єктів на ринку товарів і послуг. Жодний правил хорошого ділового тону і чесної економічної конкуренції вказаний метод не порушує, а тому не наражає суб'єкта проведення бенчмаркінгу на лишні загрози для його безпеки.

Вивчення європейського правового простору дозволило виявити і проаналізувати нам Європейський кодекс поведінки при бенчмаркінгу. Норми вказаного кодексу дозволили нам сформувати не лише принципи проведення бенчмакінгу для національних підприємств, а й окреслити переваги його застосування для безпеки суб'єкта господарювання.

В ході проведеного дослідження нами був сформований висновок, що бенчмаркінг є основною можливістю покращення роботи служб безпеки підприємств, за умов практично повної відсутності законодавчого визначення правил діяльності вказаних структурних підрозділів підприємства. Основної уваги на сьогоднішній день потребує питання пошуку партнерів по бенчмаркінгу, у зв'язку з чим ввадаємо за доцільне запропонувати створення єдиної всеукраїнської бази даних бенчмаркінгу. Саме вказана база могла б містити інформацію про усіх бажаючих суб'єктів господарювання, які бажають прийняти участь у цьому процесі. Доступ іноземних суб'єктів господарювання буде тільки вітатися.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Організація та управління охороною праці

на прикладі ПАТ “Тернопільміськгаз”

Відповідальний за охорону праці підприємствах інженер по охороні праці та техніці безпеки, який безпосередньо підпорядковується директору.

Згідно колективного договору зобов’язується:

1. Правильно організувати працю робітників і службовців, забезпечувати трудову і виробничу дисципліну, неухильно дотримуватисязаконодавства про працю і правил з охорони праці, умов праці і побуту.

2. Забезпечити виконання комплексних заходів для реалізації встановлених нормативів безпеки, гігієни праці та виробничого середовища, підвищення наявного рівня охорони праці, запобігання випадкам виробничого травматизму, професійних захворювань і аварій.

3. У разі нещасного випадку на роботі, або виникненні професійного захворювання керівництво товариства зобов’язане створити комісію про розслідування цього випадку, провести розслідування його і вести облік таких випадків згідно Положення про розслідування і облік нещасних випадків на виробництві.

4. При прийнятті на роботу працівника ознайомити його під розписку з умовами праці на його робочому місці небезпечних і шкідливих виробничих факторів, можливі наслідки їх впливу на здоров’я та пільги і компенсації за роботу в таких умовах відповідно до законодавства і колективного договору „Перелік професій працівників, зайнятих на роботах з підвищеною небезпекою”.

5. Забезпечити безоплатно працівників спецодягом, спецвзуттям та іншими засобами індивідуального захисту згідно галузевих норм, а також миючими, знешкоджуючими засобами.

6. Забезпечитипрання, хімчистку, знежирювання,

відновленнятаремонтспецодягу, спецвзуття, іншихзасобівіндивідуальногозахисту.

7. Забезпечити безоплатне проведення попередніх і періодичних профілактичних медичних оглядів працівників.

8. Відповідно до ст. 3 Закону України „Про охорону праці", надавати працівникам зайнятих на роботах з шкідливими умовами праці безкоштовно – забезпечувати молоком.

9. Проводити з прийнятими на роботу у товариство інструктажі (навчання) з охорони праці відповідно до „Положення про навчання з питань охорони праці" затверджено наказом Держнаглялохоронпраці від 17. 02. 1999р. за № 27 та щорічні навчання і перевірку знань працівників, зайнятих на роботах з підвищеною небезпекою.

10. В разі нещасного випадку адміністрація зобов'язується: відшкодувати працівникові в разі пошкодження його здоров'я з легкими травмами, тобто тимчасовою непрацездатністю, разову допомогу в розмірі:

– до 10 календарних днів –0,2 % середньомісячного заробітку,

– від 2 до 4 місяців –один середньомісячний заробіток,

– у випадку стійкої втрати працездатності потерпілим – виплатити йому суму визначену з розрахунку середньомісячного заробітку потерпілого за кожен відсоток втрати ним професійної працездатності,

– у разі смерті потерпілого виплатити одноразову допомогу його сім'ї в розмірі не менше п'ятирічного його заробітку, крім того не менше однорічного середнього заробітку на кожного його утриманця, а також на дитину, що народилася після його смерті.

11. У випадку виявлення при розслідуванні вини потерпілого, грубих його помилок або не виконання ним вимог нормативних актів про охорону праці, розмір одноразової допомоги може бути зменшений[26, с. 55].

Факт наявності вини потерпілого у виробничо-господарських умовах встановлюється комісією з розслідування нещасного випадку на ПАТ "Тернопільміськгаз" (табл. 4.1).

Таблиця 4. 1

Факт наявності вини потерпілого при нещасному випадку

№п/п	Порушення з боку потерпілого, які були однією з причин нещасного випадку	Розмір зменшення
1.	Виконання роботи в нетверезому стані, якщо цей стан був визнаний причиною нещасного випадку і якщо сп'яніння потерпілого не було обумовлене застосуванням в роботі технічних спиртів, наркотичних або інших речовин.	50%
2.	Неодноразове свідоме порушення вимог нормативних актів про охорону праці, за яке раніше накладалося дисциплінарне стягнення, вилучався талон попереджень або документально засвідчувалось офіційне попередження.	50%
3.	Первинне свідоме порушення вимог безпеки при обслуговуванні об'єктів і виконанні робіт підвищеної небезпеки.	40%
4.	Первинне свідоме порушення правил поводження з машинами, механізмами, устаткуванням, виконання робіт, що не є об'єктами підвищеної небезпеки.	30%
5.	Свідоме невикористання наданих засобів індивідуального захисту, передбачених правилами безпеки, якщо це порушення було: – первинним; – повторним.	 20% 40%

12. До порушників встановлюються заходи покарання порушників законодавчих і нормативних актів з охорони праці.

а) притягнення до дисциплінарної відповідальності (догана або звільнення з роботи –за недотримання правил внутрішнього трудового розпорядку):

– за ухилення працівника від проходження обов'язкового медичного огляду;

– за порушення інструкцій з охорони праці;

– за несвоєчасний вихід і ухід з робочого місця не дотримання графіків роботи;

б) притягнення до матеріальної відповідальності при наявності прямої дійсної шкоди, вини працівника в завданих товариству збитках (знищенні майна, устаткування, псування матеріалів і т. д.)

13. Створити в ПАТ “Тернопільміськгаз” комісію з питань охорони праці.Встановити вихідну допомогу в розмірі тримісячного заробітку працівникові, який змушений розірвати трудовий договір з причин невиконання адміністрацією вимог законодавства та зобов’язань колективного договору охорони праці, відповідно до ст. 7 Закону України „Про працю”.

На виконання Закону України „Про охорону праці” Державним комітетом України з нагляду за охороною праці згідно з наказом №72 від 3.08.1993 року затверджено „Типове положення про комісію з питань охорони праці„ та відповідно до наказу №135 від 28.12.1993 року –„Типове положення про роботу уповноважених трудових колективів з питань охорони праці”.

Згідно з цими документами, комісія з питань охорони праціорганізується в колективах (товариства) з кількістю працівників понад 50 чоловік за рішенням зборів співробітників та являє собою постійно діючий консультативно–дорадчий орган трудового колективу, що створюється з метою залучення його до співробітництва у сфері управління охороною праці газового господарства та формується на засадах рівного представництва від роботодавця та працівників.

Комісія з питань охорони праці:

проводить захист прав та інтересів працівників у сфері охорони праці;

– аналізує стан безпеки та умов праці на виробництві досліджуваного товариства і надає відповідні рекомендації роботодавцеві;

– має право звертатися до керівника ПАТ “Тернопільміськгаз” з пропозиціями щодо регулювання відносин у сфері охорони праці, встановлювати ступінь вини потерпілого, здійснювати контроль за дотриманням вимог законодавства з питань охорони праці (забезпечення засобами колективного та індивідуального захисту, профілактичним харчуванням), приймати участь у вирішенні конфліктних ситуацій у справі охорони праці тощо;

– очолюється головою, який обирається на її засіданні.

Члени комісії з питань охорони праці виконують свої обов’язки на громадських засадах, свої засідання (рішення) оформляють у вигляді протоколів, один раз на рік звітують про свою роботу на загальних зборах та беруть участь:

1) у розробленні колективного договору між адміністрацією та працівником (розділ „Охорона праці”);

2) у роботі постійнодіючих комісій з питань атестації робочих місць;

3) у розслідуванні нещасних випадків та інших конфліктних ситуацій з питань охорони праці тощо.

Члени комісії з питань охорони праці мають право:

1) безпосередньо перевіряти стан безпеки і гігієни праці, дотримання працівниками нормативних актів з охорони праці;

2) вносити пропозиції щодо усунення недоліків у сфері охорони праці;

3) вимагати у керівника товариства припинення роботи у разі створення загрози життю або здоров’ю працівників;

4) вносити пропозиції щодо притягнення до відповідальності працівників, які порушують нормативні акти з охорони праці;

5) бути обраними до складу комісії з охорони праці та бути представниками в судах, в яких слухаються питання щодо порушень охорони праці.

Питання звільнення або заміни членів комісії вирішуються тільки на зборах колективу. Особи, які створюють перешкоди для їх діяльності, несуть відповідальність у порядку, встановленому законодавством.

Отже, як видно з викладених матеріалів, питання охорони праці в виробничих умовах, в тому числі і на ПАТ "Тернопільміськгаз", є досить проблемними та різноманітними. Об'єднання зусиль керівництва, фахівців з охорони праці, громадськості –незаперечно, сприятиме значному покращанню умов праці поліграфічної галузі та забезпеченню ефективної профілактики виникнення різноманітних виробничих негараздів.

4.2 Організація безпечних умов праці на товаристві

Шкідливі чинники фізичної природи, до числа найбільш поширених з яких відносять: шум, вібрацію, температуру, вологість та швидкість руху повітря, освітлення, ультрафіолетове та інфрачервоне випромінювання, по праву вважають такими, що мають суттєве та незаперечне значення для забезпечення оптимальних умов виконання професійної діяльності у паливно-енергетичного комплексу [24, с. 114].

Розглянемо деякі з них.

1. Шум. Шум являє собою сукупність механічних коливань частинок пружного середовища (газу, рідини, твердого тіла) внаслідок впливу певної збуджувальної сили, що заважає сприйняттю корисних акустичних сигналів і справляє певний шкідливий або подразнювальний вплив на організм людини, знижуючи її працездатність.

Основними джерелами звуко– та шумоутворення є коливання, що виникають під час зіткнення, тертя або сковзання твердих тіл, протікання рідин, збігання газів тощо. Слід лише зазначити, що шумом, на відміну від звуку, прийнято називати неперіодичні, випадкові, хаотичні коливальні процеси, які відбуваються у пружному середовищі, натомість для звуку властива наявність періодичних, регулярних та упорядкованих коливань.

Головними фізичними характеристиками шуму, що мають фізіолого–гігієнічне значення, є його інтенсивність (кількість звукової енергії) та особливості спектрального розподілу (характер розподілу звукової енергії у певних октавних смугах акустичного діапазону). Разом з тим, ураховуючи, що з фізіологічної точки зору акустичні коливання характеризуються виникненням певних відчуттів у слуховій сенсорній системі, зумовлених змінами тиску частинок пружного середовищі, ще однією важливою характеристикою шуму слід вважати його гучність (рівень фізіологічного сприйняття інтенсивності акустичних коливань різної сили та частоти у порівнянні з певним еталонним звуком).

Найважливішою фізичною характеристикою шуму є його інтенсивність або сила, що визначається кількістю звукової енергії (енергетичний поріг звукового сприйняття складає 10 Вт/м) та залежить від величини амплітуди звукової хвилі. Причому чим більшою є ця амплітуда, тим інтенсивнішим є шум.

У разі збільшення звукового тиску збільшується і ступінь його сприйняття, з’являється больове відчуття. Існує 2 шкали вимірювання інтенсивності шуму –абсолютна і відносна. За абсолютною шкалою інтенсивність шуму можна характеризувати абсолютними значеннями тиску в паскалях (Па), за відносною, яка більш зручна і прийнятна, –у децибелах (дБ).

Орієнтовні рівні шуму, який створюють різні джерела, наведено в табл. 4.2.

Таблиця 4.2

Орієнтовні рівні шуму, який створюють різні джерела

Джерела шуму	Рівень шуму, дБ
Зимовий ліс у безвітряну погоду, ізольоване безшумне приміщення	0-5
Шелест листя	10
Шепітна розмова (на відстані 1 м)	15-20
Тиха квартира	30
Тиха сільська (дачна) місцевість	30

Читальний зал	35-40
Звичайна розмова (на відстані 1 м)	50-60
Гучна мова (на відстані 1 м)	60-80
Гучна музика	80-115
Легковий автотранспорт (на вулиці)	70-80
Вантажний автотранспорт (на вулиці)	80-100
Мотоцикл без глушника	95-105
Трамвай	80-90
Тролейбус	70-76
Залізничний потяг	90-96
Автомобільна сирена	80-100
Промислове виробництво (різні цехи)	80-100
Зліт реактивного літака (на відстані 100 м)	120
Блискавка, грім	130
Старт космічних ракет, вибухи, постріли	150-200

Загалом людина здатна відчувати акустичні коливання у межах від 16 до 20000 Гц, які, власне, і вважаються звуковими. Натомість акустичні коливання з частотою понад 20000 Гц називають ультразвуком, акустичні коливання з частотою менше 16 Гц –інфразвуком.

Ступінь сприйняття людиною звукових коливань з віком поступово знижується. Так, установлено, що більшість осіб у віці понад 50–60 років погано або зовсім не відчувають акустичні коливання з частотою вище ніж 5000 Гц. Подібне явище притаманне й особам із патологічними зрушеннями з боку слухового аналізатора або з деякими іншими захворюваннями.

2. Вібрація. Вібрація являє собою коливальні рухи, які відбуваються в механічних системах із пружними зв’язками внаслідок впливу певної збуджувальної сили.

Найпростішою, показовою як із суто фізичної, так і з фізіолого–гігієнічної точки зору, формою коливань такого роду є гармонійні, синусоїдальні коливання, які характеризуються максимальним переміщенням тіла (точки), що коливається у просторі, тобто його амплітудою, а також певною кількістю повних циклів коливань за одиницю часу, тобто частотою. Людина відчуває вібраційні коливальні рухи у достатньо великому діапазоні частот – від 0,15 до 8000 Гц. Час, за який відбувається один повний цикл

коливань, має назву періоду і є величиною, що обернено пропорційна частоті. Крім того, як важливі фізичні характеристики вібрації необхідно визначити віброшвидкість та віброприскорення.

За способом передачі на людину прийнято розрізняти загальну (передається через опірні поверхні на тіло людини, яка стоїть, сидить або лежить) та локальну (передається переважно через верхні кінцівки) вібрацію. Серед основних різновидів загальної вібрації (або вібрації робочих місць) виділяють транспортну, технологічну та транспортно–технологічну вібрацію.

Слід мати на увазі, що вплив на людину вібрації, навіть такого її різновиду, як локальна, не обмежується тільки ділянкою тіла, яка безпосередньо контактує з джерелом вібрації. З огляду на те, що тканини тіла, особливо кісткова система, добре проводять механічні коливання, останні більшою або меншою мірою впливають і на інші органи та організм загалом.

Так, внаслідок впливу високочастотної локальної вібрації виникають негативні зміни в судинах, погіршується кровопостачання тканин, порушується шкірна чутливість. Разом з тим низькочастотна локальна вібрація спричиняє переважно місцеві порушення, а також виражені патологічні зміни з боку кісткової тканини за наявності відносно незначних змін у судинах.

Крім того, під час аналізу особливостей впливу вібрації на організм людини необхідно виділяти та ураховувати чинники виробничого середовища, що суттєво посилюють ступінь її шкідливого впливу, а саме: високий ступінь важкості та напруженості праці, шум високої інтенсивності та несприятливі мікроклиматичні умови.

Тривалий вплив вібрації, поєднаний з комплексом несприятливих факторів, може призвести до виникнення стійких патологічних зрушень в організмі працівників і, як результат, до розвитку вібраційної хвороби.

3. Ультразвук. Ультразвук являє собою коливання середовища з частотою понад 20000 Гц. У сучасному виробництві ультразвук

використовується під час проведення паяння, зварювання, лудження, різання, дефектоскопії та цілого ряду інших технологічних процесів.

Виділяють наступні провідні біологічні ефекти впливу ультразвуку: термічний, механічний та фізико-хімічний. Саме вони зумовили достатньо широке використання ультразвуку в сучасному виробництві та в першу чергу в медичній практиці, відповідно для глибокого прогрівання тканин, проведення ультразвукової еходіагностики різноманітних захворювань, безкровного розтину і з'єднання тканин, а також стерилізації сироватки крові і плазмозамінників.

Внаслідок дії ультразвуку, рівень якого перевищує гранично–допустимий рівень (ГДР) незалежно від шляхів його впливу: через повітряне середовище або контактним шляхом –вельми імовірним є виникнення таких зрушень у стані здоров'я: з боку ЦНС: антено–вегетативний синдром, парестезії та парези, енцефаловегетополі – неврит; з боку серцево–судинної системи: брадикардія та гіпотонія; з боку органу слуху: суттєве зниження порогу сприймання, лабіринтопатія.

До числа основних запобіжних заходів для осіб, що працюють в умовах впливу ультразвуку, відносять: гігієнічне нормування, екранування ультразвукових джерел, застосування дистанційного управління і автоблокування для стаціонарного та портативного обладнання, використання індивідуальних засобів захисту (рукавиці з ізолюючими прокладками тощо), проведення попередніх та періодичних медичних оглядів.

4. Інфразвук. Інфразвуком називають акустичні коливання з частотою нижче 16 Гц.В основі біологічної дії інфразвуку також знаходяться термічний, механічний та фізико-хімічний ефекти. Вплив інфразвуку, що перевищує ГДР, зумовлює виникнення вираженої астенізації вищої нервової діяльності, зниження слуху, переважно в діапазоні низьких і середніх частот звукового ряду, виражене зниження працездатності, негативну дію на емоційну сферу тощо.

Найбільш ефективним і практично єдиним засобом боротьби з інфразвуком слід вважати зниження рівня його генерації безпосередньо у джерелі утворення (вибір малогабаритних конструкцій технологічного обладнання з великою жорсткістю з'єднання тощо). Доволі часто для попередження негативного впливу інфразвуку використовують заглушки та поглиначі інтерференційного типу, звукопоглинальні панелі і кожухи. Як індивідуальні засоби захисту широке поширення знаходять різноманітні антифони, вкладники та навушники.

5. Знижений та підвищений атмосферний тиск. Виробнича діяльність працівників у сучасному виробництві, як правило, відбувається в умовах впливу атмосферного тиску, близького до 760 мм рт. ст.

Проте в ряді випадків, наприклад, під час виконання робіт під водою або у водо–насичених ґрунтах, в процесі водолазних і кесонних робіт, при підводному плаванні в аквалангах, у ході медичної діяльності в барокамерах працівники можуть знаходитися в умовах підвищеного атмосферного тиску. Натомість при підйомі в гори, перебуванні над землею в літальних апаратах люди, навпаки, знаходяться в умовах впливу підвищеного атмосферного тиску.

Розглядаючи біологічну дію підвищеного атмосферного тиску, слід відзначити, що під час виконання короткочасної роботи в умовах гіпербарії відмічається певне підвищення фізичної працездатності та легка ейфорія. Разом з тим в умовах тривалого перебування під тиском, значення якого перевищують 7 атмосфер, можуть проявлятися симптоми токсичної дії деяких газів, котрі входять до складу повітря, що вдихається[26, с. 12-15].

Проте найбільш небезпечним є період декомпресії, під час якого або через певний відносно короткий відрізок часу вже в умовах нормального атмосферного тиску може розвинутися декомпресійна (кесонна) хвороба.

Отже, здоров'я основних, допоміжних та обслуговуючих працівників ТзОВ „Тафір ЛТД" у суттєвій мірі залежить від особливостей впливу багатьох чинників, що можуть суттєво знижувати його рівень, негативно

впливати на працездатність, зумовлювати виникнення професійно – зумовлених захворювань.

ВИСНОВКИ

В результаті проведеного комплексного дослідження нами було сформовано ряд висновків:

1. Аналіз поняття та складових системи безпеки підприємства дозволяє стверджувати, що на сьогоднішній день немає єдиного підходу до визначення поняття «система безпеки підприємства». Кожен із науковців висловлює власне бачення на це поняття. До структурних елементів системи безпеки підприємства відносять: наукову теорію його безпеки, політику і стратегію безпеки, засоби та методи забезпечення безпеки і, нарешті, концепцію безпеки підприємства.

Наукова теорія безпеки підприємства знаходиться в Україні на стадії формування.Політика безпеки підприємства як одна із складових системи безпеки покликана визначати загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цілей. Важливо, що для встановлення загальних орієнтирів необхідно спочатку сформулювати цілі забезпечення безпеки підприємства. Для успішного впровадження політики необхідно сформувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства. концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем.

2. Протидія загрозам і ризикам, які впливають на безпеку суб’єкта господарювання та підприємницьку діяльність в цілому потребує від персоналу підприємства не лише спеціальних умінь та навичок, а й докладної правової регламентації. І якщо для охоронної діяльності на сьогодні існують певні правові нормативи, викладені у Законі України «Про охоронну діяльність», то права та обов’язки служб безпеки суб’єктів господарювання не визначені ні на рівні закону, ні на рівні підзаконного

нормативно-правового акта. Отож, виходячи із вищевказаного, можна констатувати гостру необхідність у прийнятті окремого законодавчого акту, який би врегулював основні засади, принципи діяльності та правовий статус служб безпеки підприємств.

3. Основними функціями служб безпеки можна визначити: збір відомостей з цивільних справ на договірній основі з учасниками процесу; встановлення обставин недобросовісної конкуренції з боку інших підприємств; Збір відомостей щодо кримінальних справ; розслідування фактів розголошення комерційної таємниці підприємства; збір інформації про осіб, які уклали з підприємством контракти; пошук втраченого майна підприємства; розшук безвісти зниклих співробітників; розслідування фактів неправомірного використання об’єктів інтелектуальної власності підприємства; виявлення некредитоспроможних партнерів; виявлення ненадійних ділових партнерів; вивчення негативних аспектів ринку; збір інформації для проведення ділових переговорів; захист життя і здоров'я персоналу від протиправних посягань; забезпечення порядку в місцях проведення підприємством представницьких, конфіденційних та масових заходів; консультування та надання рекомендацій керівництву і персоналу підприємства з питань забезпечення безпеки; проектування, монтаж та експлуатаційне обслуговування засобів охоронно-пожежної сигналізації тощо.

4. Ефективне функціонування служби безпеки передбачає попереднє опрацювання багатьох питань. Серед них особливого значення набуває проектування оргструктури служби безпеки та її ресурсного забезпечення, оскільки без вирішення цих питань її діяльність взагалі неможлива.

5. Паралельно зі створенням служби безпеки її керівникам доводиться вирішувати питання управлінського характеру.Система управлінняскладається з суб'єкта, об'єкта управління, прямого і зворотного зв'язку. Суб'єктом управління службою безпеки виступають керівник підприємства,рада (комітет) безпеки підприємства та начальник служби

безпеки.Об'єктом управління (керованої підсистемою) в службі безпеки виступають її окремі співробітники та підрозділи.Об'єкт управління пов'язаний із суб'єктом управління каналами прямого і зворотного зв'язку (інформаційними каналами) . По каналу прямого зв'язку інформація у вигляді управлінських рішень надходить від суб'єкта управління до об'єкта, а по каналах зворотного зв'язку - у зворотному напрямку, сигналізуючи про стан об'єкта управління, його реакції на управлінські впливи .

6. Аналіз структурної організації служби безпеки підприємств дозволив нам встановити, що найчастіше служба складається із чотирьох підрозділів: розвідувального, контррозвідувального, штрабного та охоронного. Кожен із підрозділів може містити свою структуру, величину і чисельність якої визначають в залежності від завдань, які стоять перед службою безпеки підприємств.

7. Одниміз найбільш ефективних інструментів конкурентної розвідки є застосування бенчмаркінгу.Вказаний процес являє собою:

а) безупинний процес дослідження технологій, процесів, методів організації виробництва і збуту продукції, менеджменту в кращих компаніях партнерів і конкурентів з метою підвищення ефективності власної фірми;

б) науковий метод аналізу переваг й оцінювання конкурентних переваг партнерів і конкурентів однотипної чи суміжної галузі з метою вивчення і використання всього кращого у власній фірмі;

в) мистецтво виявляти і використовувати у своєму бізнесі те, що інші роблять краще, тобто реалізовувати на практиці принцип "від кращого до найкращого".

До основних видів бенчмаркінгу відносяться:

а) внутрішній;

б) конкурентоспроможності ;

в) функціональний;

г) загальний .

Критеріями успішного проведення бенчмаркінгу є правильно підібрана команда, глибока деталізація процесі , зацікавленість керівництва в результатах, інтеграція результатів бенчмаркінгу зі стратегічними планами розвитку.

Дехто із дослідників порівнюють бенчмаркінг із промисловим шпіонажем, та між ними все-таки є суттєва, на нашу думку, різниця. І полягає вона у тому, що бенчмаркінг вивчає досвід конкурентів, який не закритий сімома замками, тоді як промисловий шпіонаж націлений на вивідування промислових секретів та іншої таємної інформації, викриття якої неминуче завдасть шкоди підприємству-власнику. Отож, саме бенчмаркінг є основною можливістю покращення роботи служб безпеки підприємств, за умов практично повної відсутності законодавчого визначення правил діяльності вказаних структурних підрозділів підприємства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ареф'єва О. В. Планування економічної безпеки підприємств / Ареф'єва О. В., Кузенко Т. Б. – К.: вид-во Європ. Ун-ту, 2004. – 150 с.

2. Артемьев В. Контрразведывательная работа внутри фирмы // [Електронний ресурс] - Режим доступуhttp://hrliga.com/index.php?module=profession&op=view&id=313

3. Баяндин Н. И. Технологии безопасности бизнеса: введение в конкурентную разведку. Учеб.- практ. пособие. - М.: Юристь, 2002. - 320 с.

4. Безсмертний Р., Дорошенко А. Зовнішня розвідка на службі приватного підприємництва // Спостерігач. – 1995. - № 7.

5. Бекряшев А.К., Белозеров И.П. Теневая экономика и экономическая преступность. Электронный учебник. 2003. // [Електронний ресурс] - Режим доступуhttp://newasp.omskreg.ru/bekryash/sitemap.htm

6. Березин І. Промислове шпигунство, конкурентна розвідка, бенчмаркинг й етика цивілізованого бізнесу // Практичний Маркетинг. — 2005. — 22 липня. — № 101.

7. Бержье Ж. Промышленный шпионаж: Издательство «Международные отношения»; Москва; 1972.

8. Бланк И. А. Управление финансовой безопастностью предприятия / Бланк И. А. – К.: Эльга, Ника-Центр, 2004. – 784 с.

9. Боббі Майямей. Британський легіон: практика регістру індустрії безпеки // [Електронний ресурс] - Режим доступуhttp://www.security-ua.com

10. Бондарчук Ю.В., Марущак А.І. Безпека бізнесу: організаційно-правові основи. Навчальний посібник. - К.: Видавничий дім «Скіф», КНТ, 2008. - 372 с.

11. Боттон Н. Экономическая разведка и контрразведка [практическое пособие] . – М., 1994 .

12. Васильців Т.Г., Ярошко О.Р. Фінансова безпека підприємства: місце в системі економічної безпеки та пріоритети посилення на посткризовому етапі

розвитку економіки // Збірник науково-технічних праць Національного лісотехнічного університету України. -2011. – Вип. 21.2. – Ст. 132-136.

13. Васильчак С. В. Організаційно-правові засади для забезпечення системи економічної безпеки підприємства // Науковий вісник. — Львів, 2011. — Вип. 21.2. — С.136–141.

14. Вовченко В.В. Проблемы защиты информации от экономического шпионажа. / В.В. Вовченко, И.О. Степанов // [Електронний ресурс]-Режим доступу http://www.analitika.info

15. Войцех Конащук. Юридические основы деятельности польских детективных и охранных компаний в контексте законодательства ЕС // [Електронний ресурс] - Режим доступуhttp://www.security-ua.com

16. Гапоненко В. Ф. Экономическая безопасность предприятия: подходы и принципы / В. Ф. Гапоненко, А. А. Безпалько, А. С. Власков. — М.: Ось-89, 2006. — 208 с.

17. Гапоненко В.Ф., Безпалько А.А., Власков А.С. Экономическая безопасность предприятия. Подходы и принципы. - М.: Изд. „Ось-89”, 2006. – 208 с.

18. Геєць, В.М. Моделювання економічної безпеки: держава, регіон, підприємство: [Текст]: монография / В.М. Геєць, М.О. Кизим, Т.С. Клебанова, О.І. Черняк. – Х., 2006. – 240 с.

19. Горячєва К. С. Механізм управління фінансовою безпекою підприємства: Автореф. дис. канд. екон. наук: 08.06.01. – К.: НАУ, 2006. – 17 с.

20. Господарський кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. — 2003. — № 18. — Ст. 144.

21. Демидов Б., Величко А., Волощук И. Тайный фронт // Національна безпека України. — 2005. — № 7–8. — С. 17–23.

22. Деякі особливості дотримання норм закону України «Про охоронну діяльність» працівниками охорони, які застосували заходи фізичного впливу або спеціальні засоби // Бізнес і безпека. – 2013. - № 6. – С. 12-14.

23. Джаман М. О. Правові та інноваційні аспекти забезпечення економічної безпеки підприємств малого бізнесу // Інвестиційно-інноваційний розвиток економіки регіону. — К., 2010. — С. 337–343.

24. Дикань В.Л., Сивий В.Б., Воловельська І.В., Зубенко В.О. КОНСПЕКТ ЛЕКЦІЙ з дисципліни «Економічна розвідка та безпека бізнесу» // [Електронний ресурс] - Режим доступуhttp://metod.kart.edu.ua/search/subject/fid/3/bid/41/cid/5/sid/812/

25. Дмитренко Ю. Опасности и угрозы предпринимательству // Бізнес і безпека. – 2012. - № 2. – С. 42-45.

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

27. Донець Л.І. Економічна безпека підприємства / Л.І. Донець, Н.В. Ващенко. – К. : Центр учб. літ., 2008. - с. 4 - 18.

28. Драга А. Комплексное обеспечение безопасности фирмы. – М., 2003.

29. Економічна безпека: навч. посіб. / За ред. Варналія З.С. – К.: Знання, 2009. – 647 с.

30. Європейський досвід організації системи протидії економічній злочинності. Аналітична записка Національного інституту стратегічних досліджень при Президентові України // [Електронний ресурс] - Режим доступу http://www.niss.gov.ua/articles/1106/

31. Єгоров В. З історії розвитку промислового шпигунства // Дзеркало тижня. — 1994. — 31 грудня. — № 13. — С. 14.

32. Живко З. Б.. Живко М. О., Хомин О. Й. Особливості кадрового забезпечення служби конкурентної розвідки в економічній безпеці фірми // Наук. вісн. Львів, лерж. ун-ту внутр. справ.Сср. сконоічна.Зб. наук, праць / Гол. ред. Р. І. Тринько. - Л., 2006. - Вип. 1(3). - 344 с.

33. Живко З. Б . Теоретические основы формирования системы экономической безопасности предприятия / З. Б. Живко // Научный диалог. – 2013. –№ 7(19) : Экономика. Право. Политология. – С. 26–40.

34. Загорельская Т. Ю. Финансовая безопасность предприятия как объект

управления // Т. Ю. Загорельська.– Наук. праці ДНТУ. Вип. 103-4.– Донецьк, ДонНТУ, 2006.–С. 215 – 218.

35. Закон України “Про державну реєстрацію юридичних осіб та фізичних осіб — підприємців” від 15.05.2003 № 755-IV // Відомості Верховної Ради України (ВВР), 2003, N 31-32, ст. 263.

36. Закон України “Про ліцензування певних видів господарської діяльності” від 01.06.2000 № 1775-III // Відомості Верховної Ради України (ВВР), 2000, N 36, ст. 299.

37. Закон України «Про захист від недобросовісної конкуренції» від 07.06.1996 р. № 236/96 ВР // Відомості Верховної Ради України (ВВР), 1996, N 36, ст.164.

38. Закон України «Про захист економічної конкуренції» від 11.01.01 р. № 2210-III // Відомості Верховної Ради України. — 2001. — № 12. — ст. 64.

39. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV // Відомості Верховної Ради України (ВВР), 2003, N 39, ст.351.

40. Закон України «Про охоронну діяльність» від 22.03.2012 № 4616-VI // Відомості Верховної Ради України (ВВР), 2013, № 2, ст.8.

41. Закон України «Про розвідувальні органи України» від 22.03.2001 № 2331-III // Відомості Верховної Ради України (ВВР), 2001, N 19, ст.94.

42. Захаров О.І., Пригунов П. Я. Організація та управління економічною безпекою суб’єктів господарської діяльності: Навч. посібник. - К. - КНТ, 2008. – 257 с.

43. Зеркалов Д. В. Экономическая безопасность [Электронный ресурс]:Монография. – Электрон.данные. – К. : Основа, 2011. – 1 электрон.опт. диск (CD-ROM); 12 см. – Систем. требования: Pentium; 512 Mb RAM; Windows 98/2000/XP; Acrobat Reader 7.0. – Название с титульного экрана.

44. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка // Юридичний журнал. — 2003. — № 7.

45. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навч. посібник / М. І. Камлик. - К. : Атіка, 2005. - 432 с.

46. Кириченко О.А. Вдосконалення управління фінансовою безпекою підприємств в умовах фінансової кризи // Финансовые рынки и ценные бумаги, 2009. – №16. – 2009. – С. 22-28.

47. Кириченко О.А. Нормативно-правове регулювання системи економічної безпеки підприємництва // Інвестиції: практика та досвід. - 2009. - № 12. - С.31-34.

48. Кишеня В. Деловая разведка как необходимый инструмент обеспечения экономической безопасности бизнеса / Управление персоналом. - 2006. - №7.

49. Кіньов Ю. Р. Організаційно-правові та економічні основи утворення підрозділів конкурентної розвідки в системі економічної безпеки суб'єктів господарювання в Україні // Вісник економіки транспорту і промисловості. — Х., 2010. — № 29. — С. 99–103.

50. Кодекс України про адміністративні правопорушення від 07.12.84 // Відомості Верховної Ради Української РСР. — 1984; додаток до № 51. — Ст. 1122.

51. Комплексна економічна безпека підприємництва: сучасні тенденції формування та перспективи розвитку, економіко-правові аспекти: зб. матеріалів IV міжвуз. наук.-практ. конф. (27 березня 2008 р., м. Чернігів). - Чернігів : Видавництво ЧДІПСТП, 2008. - 140 с.

52. Конституція України, прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради України. - 1996.- №30.- Ст.141.

53. Королев М. И. Проблема безопасности в теории фирмы: развитие и противоречия / М. И. Королев // Вестник Волгоградского государственного университета. — 2012. — № 1 (20). — С. 53-58.

54. Кримінальний кодекс України від 05 квітня 2001 р. // Відомості Верховної Ради України. — 2001. — № 25. — Ст. 131.

55. Крысин А. В. Безопосность предпринимательской деятельности. – М., 2008.

56. Кузенко Т.Б. Тактичне і стратегічне планування економічної безпеки підприємства // Актуальні проблеми економіки. - 2004. - № 3. - С. 142-152.

57. Кузенко Т.Б., Мартюшева Л.С., Грачов О.В., Литовченко О.Ю. Фінансова безпека підприємства: навч. посіб. - Х.: ХНЕУ, 2010. - 300 с.

58. Линниченко А.Н. Служба безопасности предприятия – краткий анализ // [Електронний ресурс] - Режим доступуhttp://aupd.org/publications/132-sbp

59. Лянной Г.. Подчиняться либо защищаться? // BEST OF SECURITY. – 2008.- № 26.

60. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства : [монографія] / О. М. Ляшенко. — Луганськ: вид-во СНУ ім. В. Даля, 2011. — 400 с.

61. Мак-Мак В.П. Правовой статус службы безопасности // Частный сыск, охрана, безопасность, 1994. № 2.

62. Мартыненко И. Работа службы безопасности компании с персоналом // [Електронний ресурс] - Режим доступуhttp://hrliga.com/index.php?module=profession&op=view&id=545

63. Марченко В.В. Как обманывают потребителей охранных услуг// Бізнес і безпека. – 2013. - № 6. – С. 14-16.

64. Материалы журнала "Безопасность. Достоверность. Информация": [Електронний ресурс] - Режим доступуwww.bdi.spb.ru.

65. Мігус І. П. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання [Електронний ресурс] / І. П. Мігус, С. М. Лаптєв. — Режим доступу : http://www.economy .nayka.com.ua/index.php?operation=1&iid=821.

66. Нежданов И. Создание системы безопасности предприятия // [Електронний ресурс] - Режим доступуhttp://hrliga.com/index.php?module=profession&op=view&id=226

67. Нежданов И.. Как подобрать руководителя службы безопасности // BEST OF SECURITY. – 2008.- № 26.

68. Одинцов АЛ. Служба безопасности на предприятии. М.: Об-во "Знание" России, 1995 -64 с.

69. Ортинський В.Л. Економічна безпека підприємств, організацій та установ. – К.: Вид-во «Правова єдність». – 2009. – 260 с.

70. Основи економічної безпеки : [підручник] / [Бандурка О. М., Духов В. Є., Петрова К. Я., Червяков І. М.]. — Харків: Вид-во нац. ун-ту внутр. справ, 2003. — 236 с.

71. Основы экономической безопасности (Государство, регион, предприятие, личность) / под ред. Е. А. Олейникова. — М.: ЗАО «Бизнес-школа «ИнтелСинтез», 1997. — 288 с.

72. Папехин Р. С. Индикаторы финансовой безопасности предприятий / Р. С. Папехін.– Волгоград: Волгоградское научное изд-во, 2007.– 16 с.

73. Пекін А. Економічна безпека підприємств як економіко-правова категорія // Економіст. - 2007. - № 8. - С.23-25.

74. Податковий кодекс України від 02.12.2010 р. № 2755-VI // Відомості Верховної Ради України. - 2011. - № 13.

75. Подлужна Н. О. Організація управління ЕБП : автореф. дис. на здобуття наук ступеня. канд. екон. наук : спец. 08.06.01 «Економіка, організація і управління підприємствами» / Н. О. Подлужна. — Донецьк, 2004. — 22 с.

76. Пойда-Носик Н. Н. Ризики і джерела загроз фінансовій безпеці акціонерних товариств у сучасних умовах [Електронний ресурс] / Н. Н. Пойда-Носик. — Режим доступу : www.teologia.org.ua /20110920172 /statti/ dokladi /riziki-i-djerela-zagroz-finansoviie-bezpeci-akcionernix-tovaristv-u-suchasnix-umovax-172.html

77. Программа MBA-Start Модуль «Экономика и право»Тема: «Основы безопасности бизнеса».УЧЕБНИК // [Електронний ресурс] - Режим доступу http://www.wisp.ru/

78. Разнообразие частной охранной деятельности // [Електронний ресурс] - Режим доступуhttp://op-svet.ru/54-raznoobrazie-chastnoy-ohrannoy-deyatelnosti.html

79. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур: Монографія - Л.: ЛБІНБУ, 2004. -195 с.

80. Скібіцька Л.І. Економічна розвідка в антикризовому управлінні підприємством // Науковий вісник Херсонського дердавного університету. Серія «Економічні науки». – 2013. - Випуск 2. – С. 64-69.

81. Слепцов В.І. Інформаційна та економічна безпека діяльності підприємства. – К., 2010. – 248 с.

82. Служба безопасности. М: Гелеос, Л.Г. Информэтин Групп, 1998 - 525 с.

83. Солнышков О.В. Специальная правоспособность субъектов частной детективной и охранной деятельности // Журнал российского права. 2001. № 5.

84. Соловьев И.Н. Информационная и правовая составляющие безопасности предпринимательской деятельности // Налоговый вестник. - 2002. - № 10.

85. Соснин А.С., Пригунов П.Я. Менеджмент безопасности предпринимательства. Учебное пособие. – К. Издательство Европейского университета, 2002 – 504 с.

86. Способы защиты от экономического шпионажа // [Електронний ресурс] - Режим доступу http://dehack.ru

87. Судакова О. І. Стратегічне управління фінансовою безпекою підприємства / О. І. Судакова // Економічний простір.– 2008.– № 9.– С. 140 – 148.

88. Ткачук Т. Характерні особливості конкурентної розвідки та промислового шпигунства // [Електронний ресурс] - Режим доступуhttp://www.personal.in.ua/article.php?ida=451

89. Усатюк А. Создание на предприятии службы безопасности // [Електронний ресурс] - Режим доступуhttp://hrliga.com/index.php?module=profession&op=view&id=1085

90. Фастенко А.А. , Жиляєв В. І. Організаційно-правові засади приватної охоронної діяльності : практичні поради діловим людям . М. : РНСЕБ , 1993. – 156 с.

91. Цивільний кодекс України від 28 листопада 2001 р. // Голос України. – 2003. - № 45-46. – 12 березня. - № 47-48. – 13 березня.

92. Чередниченко А.О. Методи забезпечення захисту підприємств від економічного шпигунства // Вісник економіки транспорту і промисловості. – 2013. - № 42. – С. 335-338.

93. Чистоклетов Л.Г. Інформація як визначальний чинник адміністративно-правового забезпечення фінансово-економічної та інформаційної безпеки суб'єктів господарювання /Л.Г. Чистоклетов. // Митна справа. - 2011. - № 5, ч. 2. - С.441-448.

94. Шаваев А.Г. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы. – М.: Концерн "Банковский деловой центр", 1998.

95. Шевченко СВ., Шестаков В.И. Каким видится законодательство о частной охранной и детективной деятельности в начале III тысячелетия // Государство и право. 2000. № 4.

96. Шумилин А.Ю. Частное детективное и охранное право. М., 1999.

97. Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. М.: "Ось-89", 1995-114 с.