Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _Навчально-науковий центр заочної форми навчання_____
(повна назва)
Кафедра_економічної кібернетики та управління економічною безпекою____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти_____другий (магістерський)_____

_____Організація захисту комерційної таємниці в системі економічної ___
_____безпеки підприємства_____
(тема)

Виконав:
студент _2_ курсу, групи УФЕБизм-20-1_____
_____Сеїдова Гюльнара Мірсаттар кизи____
(прізвище, ініціали)

Спеціальність 073 Менеджмент_____
_____
(код і повна назва спеціальності)
Тип програми _освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма __Управління_____
фінансово-економічною безпекою_____
(повна назва освітньої програми)

Керівник __проф. Полозова Т.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ __Полозова Т. В._____
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет _Навчально-науковий центр заочної форми навчання_____
(повна назва)
Кафедра_економічної кібернетики та управління економічною безпекою____
(повна назва)
Рівень вищої освіти _другий (магістерський)_____
Спеціальність 073 Менеджмент_____
(код і повна назва)
Тип програми_освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові__Сеїдовій Гюльнарі Мірсаттар кизи_____
(прізвище, ім'я, по батькові)

1. Тема роботи_ Організація захисту комерційної таємниці в системі економічної безпеки підприємства_____
затверджена наказом по університету від 23 жовтня 2021 р. № _165 Стз_____
2. Термін подання студентом роботи до екзаменаційної комісії _14 грудня 2021 р._____
3. Вихідні дані до роботи Наукові інформаційні джерела, періодичні видання, теоретичні та методичні розробки вчених в області забезпечення фінансово-економічної безпеки підприємств, статистичні дані досліджуваного підприємства_____
4. Перелік питань, що потрібно опрацювати в роботі_____
Вступ. 1. Теоретичні засади організації захисту комерційної таємниці на підприємстві. 2. Аналіз господарської діяльності та організації захисту комерційної таємниці на ТОВ «Стем». 3. Удосконалення організації захисту комерційної таємниці в системі економічної безпеки підприємства. Висновки. Перелік джерел посилання. Додаток.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій_____
1. Об'єкт, предмет, мета і завдання дослідження. 2. Класифікація даних, що належать до комерційної таємниці. 3. Способи втрати комерційної таємниці. 4. Основні показники діяльності ТОВ «Стем». 5. Структура витрат за економічним елементами. 6. Динаміка витрат підприємства. 7. Функції, що покладаються за службу безпеки. 8. Перелік відомостей, що становлять комерційну таємницю. 9. Заходи щодо роботи з кадрами та запобіганню шпигунству. 10. Етапи процесу організації захисту інформації за методом «OPSEC». 11. Матриця відповідальності. 12. Класифікація ризиків проекту захисту комерційної таємниці на підприємстві._____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	25.10.21-01.11.21	виконано
2	Виконання другого розділу роботи	02.11.21-10.11.21	виконано
3	Виконання третього розділу роботи	11.11.21-30.11.21	виконано
4	Оформлення роботи	01.12.21-05.12.21	виконано
5	Перевірка роботи на плагіат	06.12.21-08.12.21	виконано
6	Підготовка доповіді та ілюстративного матеріалу	09.12.21-10.12.21	виконано
7	Рецензування роботи	11.12.21-13.12.21	виконано
8	Подання роботи до екзаменаційної комісії	14.12.2021	

Дата видачі завдання _25 жовтня 2021 р._

Студент _____
(підпис)

Керівник роботи _____ __проф. Полозова Т.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 94 с., 6 табл., 10 рис., 77 джерел, 1 додаток.

КОМЕРЦІЙНА ТАЄМНИЦЯ, ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ, СЛУЖБА БЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, ЕКОНОМІЧНА РОЗВІДКА І КОНТРРОЗВІДКА.

Об’єктом дослідження є управління системою економічної безпеки підприємства.

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій щодо удосконалення організації захисту комерційної таємниці в системі економічної безпеки підприємства.

Розкрито змістовний контент поняття «комерційна таємниця». Розглянуто особливості захисту комерційної таємниці в умовах конкуренції. Здійснено аналіз господарської діяльності та організації захисту комерційної таємниці на ТОВ «Стем». Запропоновано напрями організаційного забезпечення захисту комерційної таємниці на підприємстві. Розроблено заходи щодо удосконалення організації захисту комерційної таємниці на ТОВ «Стем». Запропоновано рекомендації щодо розробки проекту захисту комерційної таємниці на основі системного методу «OPSEC».

ABSTRACT

Master thesis: 94 p., 6 tables, 10 fig., 77 sources, 1 exhibit.

COMMERCIAL SECRET, ORGANIZATIONAL SECURITY, SECURITY SERVICE, PROTECTION OF INFORMATION, ECONOMIC INTELLIGENCE AND COUNTER-INTELLIGENCE

The object of research is the management of the economic security of the enterprise.

The purpose of the research is the theoretical justification and development of practical recommendations for improving the organization of protection of trade secrets in the economic security of the enterprise.

The meaningful content of the concept of «trade secret» is revealed. Features of protection of a trade secret in the conditions of competition are considered. The analysis of economic activity and organization of protection of trade secrets at «Stem» LLC is carried out. The directions of organizational maintenance of protection of a trade secret at the enterprise are offered. Measures have been developed to improve the organization of trade secret protection at «Stem» LLC. Recommendations for the development of a project for the protection of trade secrets based on the system method «OPSEC» are offered.

ЗМІСТ

ВСТУП

Сьогодні в Україні в процесі підприємницької діяльності, зі створенням нових технологій в результаті інтелектуальної праці виникають інформаційні об’єкти, що набувають комерційної цінності. Це можуть бути методи роботи, перспективні технічні рішення, результати маркетингових досліджень тощо, спрямовані на досягнення успіху бізнесу.

Проте не менш важливим фактором, який продовжує супроводжувати певне економічне середовище, є злочинна поведінка та інші обставини, що ускладнюють або знищують поведінку підприємців. Наявність умов, що спричиняють реальну загрозу шкоди (збиток) суб’єктам господарювання, висуває ряд пріоритетних та довгострокових завдань, які потребують швидкого вирішення, а саме – питання економічної безпеки.

З розвитком ринкових відносин комерційна діяльність в країні здійснюється в умовах дедалі більш невизначеного та нестабільного економічного середовища. Факти довели, що в отриманні очікуваних кінцевих результатів існують невизначеності, тому збільшується ризик, тобто ризик невдачі та непередбачених збитків. Особливо це актуально на початкових етапах розвитку бізнесу.

У нових ринкових та конкурентних умовах постає багато проблем не лише забезпечення безпеки фізичних та юридичних осіб та їх майна, а й забезпечення безпеки комерційної (комерційної) інформації як виду інтелектуальної власності. Як закони, так і спеціальні заходи використовуються для захисту потоку ділової інформації від різних порушень і для захисту її складних застосувань, коли це необхідно. Це визначає актуальність теми даної роботи.

Проблеми організаційного забезпечення захисту комерційної таємниці на підприємстві висвітлювалися у роботах таких авторів, як: Л.Є. Довгань,

А.В. Козаченко, І.П. Отенко, П.Я. Пригунов, С.І. Пучков, Н. Й. Реверчук О.В. Малик та багато інші.

Об’єктом дослідження є управління системою економічної безпеки підприємства.

Предметом дослідження є організаційне забезпечення захисту комерційної таємниці на підприємстві.

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій щодо удосконалення організації захисту комерційної таємниці в системі економічної безпеки підприємства.

Для досягнення мети були поставлені такі задачі:

– розкрити змістовний контент поняття «комерційна таємниця»;

– розглянути особливості захисту комерційної таємниці в умовах конкуренції

– здійснити аналіз господарської діяльності та організації захисту комерційної таємниці на ТОВ «Стем»;

– запропонувати напрями організаційного забезпечення захисту комерційної таємниці на підприємстві;

– розробити заходи щодо удосконалення організації захисту комерційної таємниці на ТОВ «Стем»;

– запропонувати рекомендації щодо розробки проекту захисту комерційної таємниці на основі системного методу «OPSEC».

Інформаційною базою дослідження були періодичні видання в межах предметної області, наукові праці різних авторів, законодавчі акти України, бухгалтерська і статистична звітність досліджуваного підприємства.

У процесі дослідження використані методи: аналізу та синтезу, за допомогою яких досліджені організаційно-правові аспекти забезпечення захисту комерційної таємниці на підприємстві; теоретичного пошуку – для дослідження наукової проблематики та вивчення досвіду закордонних і вітчизняних вчених; системного підходу – для дослідження систем

зовнішнього та внутрішнього середовища, що впливають на результати діяльності підприємства; фінансового аналізу, зіставлення – для узагальнювання показників господарської діяльності досліджуваного підприємства; графічний – для наочного представлення результатів дослідження; статистичні – з метою дослідження діяльності підприємства.

Практична значущість отриманих результатів полягає у тому, що запропоновані рекомендації можуть бути використані на підприємствах різних форм власності з різними обсягами виробництва. Запропоновані рекомендації дозволяють поліпшити організацію захисту комерційної таємниці на підприємстві, що підвищить ефективність прийняття управлінських рішень в області управління системою фінансово-економічної безпеки підприємства. Практичне значення мають розроблені заходи щодо підвищення якості забезпечення захисту комерційної таємниці на підприємстві. Можливими об’єктами практичного використання результатів дослідження можуть бути комерційні та некомерційні підприємства будь-якої форми власності та різних видів діяльності, посередницькі організації, фінансово-кредитні установи, страхові організації.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на ІІ Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків, 2021).

Публікації. Результати досліджень, проведених у роботі, опубліковано у 2 наукових працях, у тому числі 1 стаття у колективній монографії та 1 тези конференції.

1 ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

1.1 Змістовний контент поняття «комерційна таємниця»

Останнім часом інформація та знання відіграють вирішальну роль у всіх сферах людської діяльності та стають основними чинниками економічного розвитку. У зв’язку зі зростанням попиту на інформацію та розвитком галузі інформаційних послуг значення інформації як товару зростає з кожним днем. Це підтверджує зростання внеску інформаційного сектора у створення національного багатства. В умовах посилення тиску ринкової конкуренції, як невід’ємної частини маркетингової інформаційної системи компанії, особливу увагу слід приділяти дотриманню комерційної таємниці. Тому вивчення питання отримання та захисту інформації як комерційної таємниці є актуальним завданням прикладної економіки сьогодні.

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою та використанням різноманітних інформаційних потоків.

У розвинених країнах більшість компаній і підприємств дуже стурбовані цим важливим питанням. В Україні у розвитку та становленні малого та середнього підприємництва особливого значення набула проблема витоку важливих корпоративних даних.

В умовах ринкової конкуренції для отримання вигоди використовуються різноманітні методи, у тому числі збір інформації від інших організацій. Дедалі частіше трапляються випадки незаконних методів, що посилює загострення конкуренції. Адже важко, а іноді й неможливо бути конкурентоспроможним без розуміння поведінки конкурентів, очікуваного попиту на їхню продукцію та перспективних досліджень.

Якщо інформація має реальну чи потенційну комерційну цінність, є службовою чи комерційною таємницею та не може бути вільно отримана з правових причин, власник інформації вживає заходів для захисту її конфіденційності. Інформація, яка не може бути використана як службова чи комерційна таємниця, регулюється законодавством та іншими нормативно-правовими актами (це статут і складові документи підприємства, ліцензії, патенти, податкові документи, кількість і склад працівників, їх заробітна плата, екологічна продукція, реалізація продуктів, порушення антимонопольного законодавства, інформація про майно та розмір готівки тощо). Тому дуже важливо з’ясувати природу комерційної таємниці.

Згідно з економічним глосарієм, комерційна таємниця – навмисно прихована з комерційних цілей, економічних інтересів, а також інформація про виробництво, економіку, управління, науку, техніку та фінансову діяльність пов'язаних осіб і компаній, а також їх захист здійснюється через конкуруючі інтереси та економічні Можливі загрози безпеці [1]. Коли комерційні інтереси тісно пов’язані з комерційною таємницею, виникне комерційна таємниця.

У повсякденному житті частіше вживається термін «комерційна таємниця», але насправді це синонім комерційної таємниці. Комерційна таємниця охороняється законом. Це право підприємств та підприємців засекречувати (обмежувати доступ до інформації) відомостей про компанії та корпоративну діяльність, а поширення такої інформації може завдати шкоди їхнім інтересам [2].

Компанії та підприємці мають право зберігати в таємниці всі аспекти своєї діяльності, поширення цієї інформації послаблює їх позиції на ринку, а отже, викличе інтерес у конкурентів.

Конфіденційність підприємства – це в основному виробничі секрети організації про результати досліджень, проектування та технічні дослідження, а також конкретні рішення випадкових проблем у виробничому

процесі. Це може бути інформація про виробництво, проектування та підготовку до запуску нових продуктів, витрати, орієнтовні ціни та методи та методи організації виробництва.

Це також спеціальні технічні рішення, пов'язані з методами управління конкретними виробничими (господарськими) процесами. Нарешті, до комерційних аспектів секретів відноситься підготовка та укладання різноманітних угод, а також попередні переговори між учасниками.

Інформація є товаром у ринковій економіці, і її отримання, зберігання, передача та використання мають підкорятися законам ринкової економіки. Комерційна таємниця є власністю підприємств.

Можна з упевненістю сказати, що його метою є надання підприємствам економічної переваги в конкурентній боротьбі.

Інформація, що становить комерційну таємницю, повинна відповідати низці вимог [3]:

– публічне використання інформації пов'язане із заподіянням шкоди підприємству;

– з правових причин інформація не є загальновідомою або загальнодоступною;

– компанія зможе вжити відповідних заходів для збереження конфіденційності з міркувань економічних чи інших інтересів;

– інформацію потрібно захищати, оскільки вона не є державною таємницею і не захищена законодавством про авторське право та патенти;

– приховування цієї інформації не зашкодить суспільству.

Намагаючись захистити інформацію, що охоплюється комерційною таємницею, компанія змушена вирішувати подвійну проблему: з одного боку, вона повинна рекламувати свою продукцію (послуги), щоб інформувати постачальників і споживачів про свою діяльність, з іншого боку – діє за відсутності конкретної інформації. У разі реклами це розкриє багато аспектів

діяльності компанії, що неможливо – компанія стикається з проблемою витоку комерційної таємниці.

Класифікація даних, що належать до комерційної таємниці підприємства наведена на рис. 1.1 [3] .

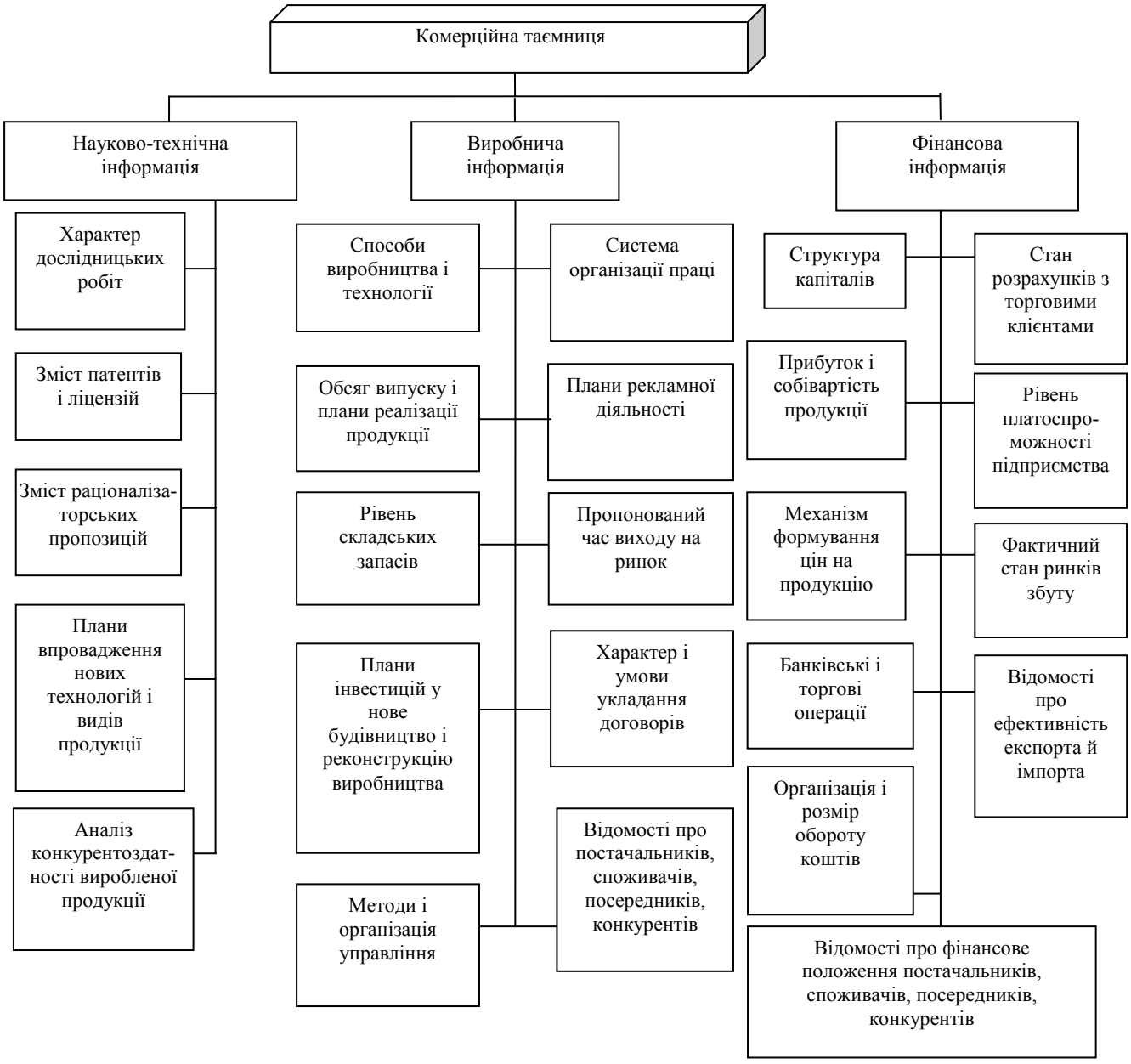

Рисунок 1.1 – Класифікація даних, що належать до комерційної таємниці підприємства

Розпочати бізнес без конкуренції неможливо. Реалізація останнього може приймати різні форми, включаючи крадіжку або збір інформації інших

людей, відомих як шпигунство. З цією проблемою вже стикаються підприємці. З одного боку, вони змушені захищати свої таємниці (цінну інформацію), з іншого боку – намагаються захопити секрети своїх конкурентів, щоб отримати перевагу в ринковій конкуренції.

Фахівці в галузі стратегічного планування та управління виробництвом включають збір інформації про конкурентів для рутинного маркетингу, а також інформацію про потенційних споживачів, репутацію компанії, державний нагляд за ринком тощо [4-5].

За даними Нью-Йоркського дослідницького центру, в галузі економіки збір інформації в основному поділяється на три сфери [2]:

– ринкова інформація;

– інформація про виробництво;

– інформація про організаційні характеристики та фінанси.

Ці сфери охоплюють майже всі аспекти діяльності підприємства. У цих сферах практично неможливо спробувати захистити комерційну таємницю шляхом обмеження доступу до інформації, але в цьому відношенні необхідно боротися з конкурентами на ринку. Адже об’єктами економічного інтелекту найбільше слідкують технологічно розвинені галузі та їх лідери. Методи, за допомогою яких економічний авангард отримує додатковий пріоритет, є не тільки об’єктом пильної уваги, але й викликають бажання інших суб’єктів господарювання до цих методів.

Поява різних шляхів отримання додаткових благ – це весь процес економічного прогресу. Нерівність доходів і додаткові пільги є основою для формування економічної таємниці, тобто інформації про шляхи отримання додаткових пріоритетів. Якщо їхня поява створює таємницю, останнє викличе бажання певних людей та власників таємниці володіти нею – зберігати й захищати її [2].

Слід зазначити, що найкраще збирати інформацію в рамках ділового етикету. Іншими словами, спочатку законно, а потім точно збирати

інформацію, яка може просуватися з прогресом, але не зашкодить іншим компаніям, суспільству тощо.

Як і будь-яка діяльність, економічне шпигунство (розвідка) потребує певних інструментів. Колекція засобів визначається способом пошуку та отримання необхідної інформації, що в кінцевому підсумку визначає ефективність усієї розвідувальної роботи. Усі методи збору інформації можна розділити на легальні, напівлегальні та нелегальні. Якщо ви купуєте в магазині і отримуєте інформацію про товар конкурента, виконуючи вівісекцію зразка у власній лабораторії, то це цілком законний метод і не несе жодної відповідальності. Якщо конфіденційна інформація конкурента отримана через його постачальника, цей метод не несе жодної відповідальності, крім етики та етики, і може бути класифікований як напівлегальний. Якщо файл викрадено, такий спосіб отримання інформації є незаконним і може призвести до кримінальної чи іншої юридичної відповідальності.

Збір інформації з юридичних каналів має здійснюватися у сфері фінансів, виробництва, досліджень, управління, маркетингу та людських ресурсів. Дуже ефективним методом збору правової інформації є участь експертних агентів із залученням офіційних іноземних представництв – посольств, консульств, торгових та інших представників.

Напівлегальні методи збору інформації найчастіше впливають на етику, етику управління та підприємницький дух міжособистісних стосунків. Це можуть бути розмови з конкурентами, конкурси, запрошення до консультантів, використання коштів і суспільства, наукові контакти, заманювання провідних експертів.

Незаконні методи збору розвідувальних даних передбачають конфіденційну інформацію, захищену власником, як правило, захищену законом. У наукових публікаціях вітчизняних авторів також подано (і

детально проаналізовано) систематизований перелік можливих шляхів несанкціонованого доступу до конфіденційної інформації.

Сюди входять, наприклад: активна співпраця, допит, розвідка, підслуховування переговорів різними способами, таємне отримання інформації та документів, викрадення, копіювання, підробка (модифікація), саботаж (знищення, саботаж), незаконні канали зв'язку та лінії зв'язку. Передача, перехоплення, візуальне спостереження, фотографування, збір і аналіз і обробка» [5].

Щодо можливих методів отримання комерційної інформації від інших компаній, слід підкреслити, що 90-95% усієї необхідної інформації можна отримати через легальні канали [5]. Іншу інформацію (зазвичай найціннішу і надійно захищену) промислові шпигуни надають притаманними їм методами, такими як крадіжка документів і зразків нової продукції, вимагання, підкуп працівників компаній-конкурентів, прослуховування, розслідування та оптичне спостереження, несанкціоноване. має право підключатися до комунікаційних систем, мереж і комп’ютерних мереж, розсилання та наймання агентів і навіть очищення суб’єктів від конкурентів або їх бізнесу.

Згідно з іншими джерелами, «приблизно 80% інформації американських спецслужб надходить із таких джерел, як дипломати-шпигуни, військові аташе, іноземні ЗМІ та репортажі, довідники, офіційні заяви уряду, документи та плани, історії та матеріали з подорожей» [2].

Серед відповідних державних установ промислово розвинених країн існують спеціальні посередницькі служби, які надають клієнтам певні види ділової інформації про компанії, які їх цікавлять. З розвитком промислового шпигунства різноманітні методи захисту підприємницької таємниці постійно вдосконалюються.

Успішний розвиток підприємництва залежить насамперед від політичного та економічного середовища, в якому воно знаходиться, але не

можна забувати й про ситуаційні фактори, які можуть серйозно перешкоджати підприємницьким діям. Реальна загроза заподіяння шкоди суб'єктам господарювання ставить перед собою багато першочергових і довгострокових завдань, які потребують швидкого вирішення, а саме – питання економічної безпеки. Багато спірних питань пов'язані національним законодавством, але не всі.

В умовах жорсткої конкуренції завжди виникає багато проблем. Вони піклуються про захист потоку інформації від різного роду порушень. Підприємці, які займаються рекламою, повинні знати, що конкуренти можуть заблокувати його ідеї на етапі тестового маркетингу. Коли підприємство використовує добре відомі методи виробництва, технології, обладнання тощо та отримує високі прибутки – хоча такі дані є загальнодоступними, сам факт їх використання є комерційною таємницею. Деякі підприємства виграють від монополії ринку, тобто в регіоні не вистачає виробників подібної продукції. Немає необхідності зневажати заходи щодо своєчасного захисту комерційної таємниці, адже завдяки вільному доступу до необхідних даних навіть малі підприємства можуть швидко організувати подібне виробництво та конкурувати.

У більшості випадків витік інформації компанії відбувається з ініціативи співробітників шляхом підкупу, помсти та необережного використання важливих даних. Комп'ютеризація бізнес-структури, накопичення різноманітної інформації та її допомога полегшують пошук і пошук інформації про конкурентів.

У більшості випадків люди, які хочуть використовувати цю інформацію, є обслуговуючим персоналом, у тому числі недобросовісними, які мають намір використовувати інформацію, якою володіють, для продажу іншим або в особистих цілях з метою отримання прибутку.

Тому на користь конкурентів діють дії, які можуть бути притягнені до відповідальності за законом: шахрайство, саботаж, пошкодження комп’ютера. За оцінками експертів, американські компанії щороку втрачають

понад 4 мільярди доларів США через розкрадання виробничої та комерційної таємниці [2, с. 78]. Крім відвертої крадіжки, може статися і витік інформації. Найімовірнішими джерелами є: особи, які мають доступ до інформації, файли, що містять цю інформацію, технічні засоби та системи обробки інформації, у тому числі лінії зв'язку для передачі інформації.

Тепер компаніям необхідно захищати важливі дані, що стосуються комерційної таємниці, а також достовірну інформацію про конкурентів, щоб визначити нові переваги та сприятливі умови для подальшої роботи.

В економічній літературі зосередьтеся на етиці, яка підтримує чесний бізнес. У ході конкуренції, як складової ринкової економіки, використання промислового шпигунства не можна віднести до етичного типу підприємницьких ділових відносин.

Проте, як показала зарубіжна практика, без економічного, промислового, науково-технічного та інших видів шпигунства конкуренція на ринку немислима.

Однак найбільш сприятливе соціально-економічне середовище для розвитку підприємства не завадить банкрутству, якщо конфіденційна інформація компанії (компанії) буде викрадена внаслідок успіху шпигунства. Шпигунство – це тінь ринкової конкуренції, двигун одних компаній і гальмо інших. Тому ми помітили, що необхідно приділяти достатню увагу захисту інформації на підприємстві, а також усіх інших функцій і видів діяльності.

1.2 Особливості захисту комерційної таємниці в умовах конкуренції

Актуальність цього дослідження полягає в тому, що будь-яка господарська діяльність пов'язана з використанням певного обсягу інформації, але не вся інформація, що циркулює в економіці, є загальнодоступною, частина якої є конфіденційною та міститься в

комерційній таємниці. Варто підкреслити подвійну важливість комерційної таємниці за ринкових умов. Тому, з одного боку, комерційна таємниця є ознакою будь-якого підприємства, що робить його виробництво більш індивідуальним та ефективнішим, ніж середньогалузевий.

З іншого боку, інформація, що має статус комерційної таємниці на підприємстві, призведе до незнання інших підприємств та відсутності інформації щодо управлінських рішень та загалом спричинить ринкову невизначеність. Слід підкреслити, що питання інформаційного змісту як комерційної таємниці є дискусійним, оскільки не існує єдиного способу визначення цього терміну. У літературі часто зустрічаються такі поняття, які стосуються комерційної таємниці, як «комерційна таємниця», «таємниця виробництва», «виробничі секрети», «конфіденційна інформація» тощо [22, 23].

Слово «інформація» в Законі України означає записи або публічно оприлюднену інформацію про події та явища, що відбулися в суспільстві, країні та навколишньому середовищі [16]. Це визначення є дуже широким і тому потребує більш детального розгляду. У Законі України «Про захист економічної конкуренції» [17] визначення поняття «інформація» більш детальне: це будь-які форми та форми, що зберігаються на будь-яких носіях (включаючи листи, книги, нотатки, ілюстрації (карти, схеми, організаційна структура) рисунки, креслення, схеми тощо), фотографії, голограми, фільми, відео, мікрофільми, звукозаписи, бази даних комп’ютерних систем або всі або частина їх елементів), пояснення персоналу та будь-яка інша публічно оголошена чи записана інформація.

Щодо поняття «комерційна таємниця», то його часто асоціюють із засобами запобігання недобросовісній конкуренції при реалізації прав інтелектуальної власності. Відповідно до господарського кодексу України, до об'єктів інтелектуальної власності у сфері управління відноситься комерційна таємниця. Зокрема, комерційною таємницею може бути визнана недержавна

таємниця, пов’язана з виробництвом, технологією, функціонуванням, фінансовою та іншою діяльністю підрозділу, якщо розголошення може завдати шкоди інтересам підрозділу [37].

Більшість документів, що стосуються доповідей з питань комерційної таємниці та правових напрямків, тобто авторів, які оскаржують зміст поняття, мають різне тлумачення окремих законів України. Це пояснення є дещо одностороннім.

Тому метою цього дослідження є аналіз подвійного значення комерційної таємниці в умовах конкуренції та ринкової невизначеності.

Зі вступом України до Світової організації торгівлі (СОТ) та подальшою глобалізацією економіки, коли загострюється конкуренція між вітчизняними виробниками, і на внутрішній ринок виходить все більше міжнародних конкурентів, успіх чи невдача кожного підприємства та його конкурентоспроможність залежать від ефективності виробництва, яке вимірюється рівнем задоволення потреб споживачів. Щоб вижити в жорсткій конкуренції та викликати інтерес споживачів до своєї продукції, менеджерам майже щодня доводиться приймати ключові рішення, головна умова – мати якомога повнішу та достовірну інформацію. Однак інформація, як і інші економічні ресурси, завжди обмежена і суперечлива, тому підприємницька діяльність будь-якого підприємства здійснюється в умовах неповної та недостовірної інформації, тобто в невизначених умовах. Це в свою чергу призведе до загрози відхилення фактичних результатів від плану, ризику втрати ринкової конкуренції, переходу лояльних споживачів до конкурентів. Тому менеджерам необхідно враховувати вплив невизначеності та ризики для корпоративної діяльності.

Невизначеність визначається як відсутність достовірної інформації або інформації про стан економічної діяльності та низький ступінь передбачуваності цих умов. Крім того, невизначеність є невід'ємною ознакою ринкового середовища, оскільки на ринкову кон'юнктуру впливають різні

фактори, які не оцінюються загалом, такі як: економічна та ринкова кон'юнктура; державна діяльність; структурні зміни; технологічний прогрес; природа та екологічні компоненти; забезпечення ресурсами; тенденції демографічної ситуації населення; соціальна та культурна складові; можлива сфера стратегічного планування; міжнародне середовище тощо [25-28].

Однак слід зазначити, що сама компанія не має наміру викликати ринкову невизначеність і приховувала власні комерційні таємниці від суб'єктів недобросовісної конкуренції. Неоднозначність комерційної таємниці подана на рис. 1.2.

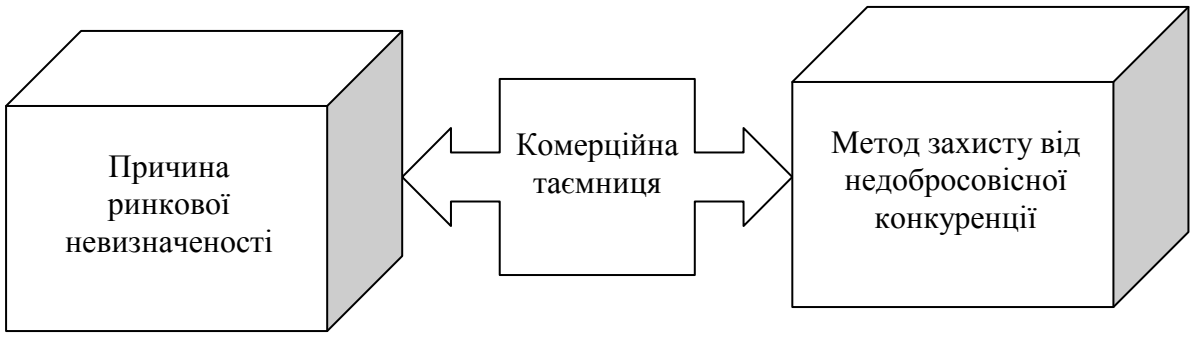

Рисунок 1.2 – Двозначна природа комерційної таємниці підприємства

Внутрішнє законодавство визначає недобросовісну конкуренцію як будь-який акт конкуренції, який порушує правила ведення бізнесу, торгівлю та інші чесні практики. До таких дій, зокрема, належать такі [14]:

– незаконне збирання, розголошення та використання комерційної таємниці;

– незаконний збір інформації, що становить комерційну таємницю (не включаючи інформацію, отриману з відкритих джерел або шляхом дослідження ринку);

– розголошення комерційної таємниці;

– схильність до розголошення комерційної таємниці;

– незаконне використання комерційної таємниці;

– тому подібне.

У таблиці 1.1 більш детально пояснюється суперечливе значення комерційної таємниці як причини ринкової невизначеності та методів запобігання недобросовісній конкуренції.

Таблиця 1.1 – Суперечливе значення комерційної таємниці

Критерій порівняння	Комерційна таємниця як причина ринкової невизначеності	Комерційна таємниця як предмет уваги конкурента
Суб'єкт	Підприємство – власник комерційної таємниці	Конкурент підприємства власника комерційної таємниці
Об'єкт	Комерційна таємниця	Комерційна таємниця
Дія суб'єкта над об'єктом	Прагне зберегти	Прагне заволодіти
Метод	Свідомий активний і пасивний захист інформації	Методи недобросовісної конкуренції (шпигунство тощо)
Мета	Збереження комерційної таємниці як запоруки власної конкурентоспроможності	Отримати секретні дані іншого підприємства та скористатися ними для зміцнення позицій власного підприємства

Наявність комерційної таємниці в діяльності будь-якого підприємства є притаманною йому характеристикою, а невизначеність зовнішнього середовища, в якому працює підприємство, – характеристикою ринкових відносин. Як зазначалося вище, компанії та їхні комерційні таємниці не є єдиною причиною такої невизначеності на ринку. Невизначеність ринку вважається його нормальним станом. Підприємства не повинні свідомо розголошувати свої комерційні таємниці для прозорості та визначеності зовнішнього середовища, інакше ринкова економіка матиме ознаки адміністративного командування.

За оцінками американських експертів, 20% втраченої інформації є причиною розорення компанії, а 60 із 100 випадків знищить компанію (організацію) протягом місяця [2]. Тому одним із головних завдань компаній, які прагнуть залишатися конкурентоспроможними, має бути ефективний захист комерційної таємниці. Необхідно пам'ятати про всі можливі шляхи та джерела втрати такої інформації, адже конкуренти не тільки можуть свідомо

відшукувати конфіденційну інформацію, але й компанія може її втратити через власне недбале ставлення до комерційної таємниці. Найбільш поширені способи втрати комерційної таємниці показані на рис. 1.3.

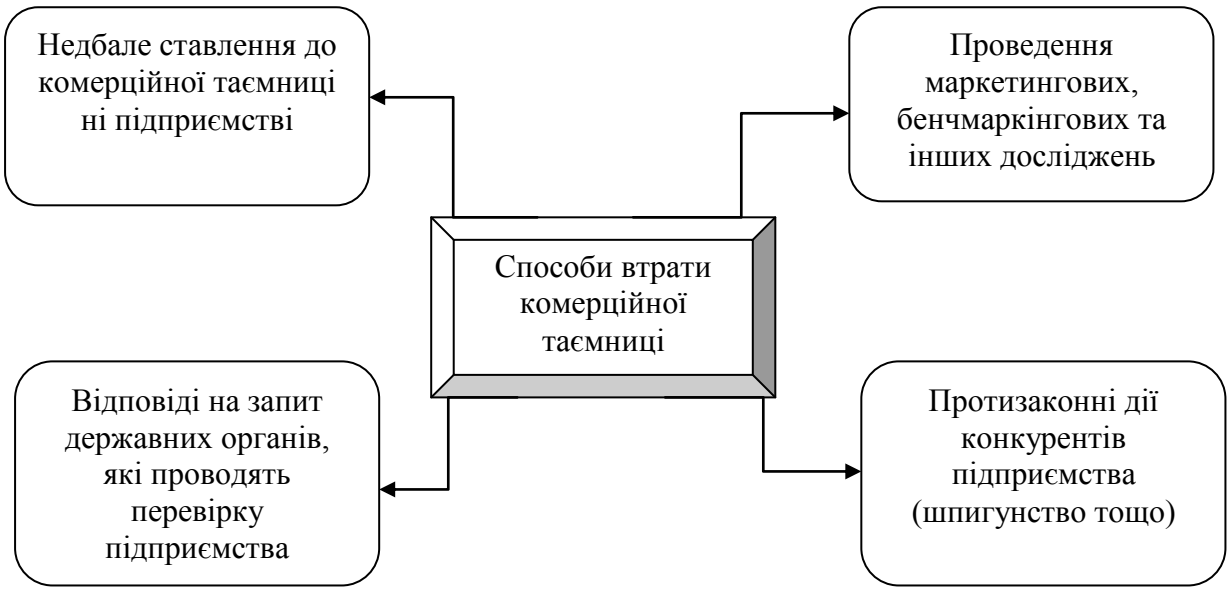

Рисунок 1.3 – Найпоширеніші способи втрати комерційної таємниці

Перш ніж продовжувати захищати комерційну таємницю, керівництво повинно чітко розуміти та визначити, яку конкретну інформацію про компанію слід перевести в стан комерційної таємниці. Практика підприємницької діяльності не лише дозволяє віднести результати інтелектуальної та творчої діяльності (наприклад, ноу-хау, спеціальні методи роботи, винаходи тощо) до комерційної таємниці, але й допускає певні факти, події та явища, які не є продуктом інтелектуальної діяльності, але є предметом комерційних та інших інтересів суб'єкта корпоративної діяльності (інформація про укладення комерційних договорів і контрактів; ділові відносини; списки постачальників і клієнтів; інформація про технічне оснащення; заробітна плата працівників тощо). Наприклад, маючи інформацію про господарські операції, легко зрозуміти виробничий і фінансовий стан підприємства.

У бізнесі використовуються два види інформаційної безпеки. Це так званий активний і пасивний захист інформації [27].

Пасивний захист означає, що власник інформації, власник патенту або авторського права, надає доступ всім відповідним сторонам, але ці люди не можуть використовувати її в комерційних цілях, оскільки власник має виключне право дозволяти комусь іншим чином використовувати цю інформацію. Отже, у разі несанкціонованого використання інформації захист інтересів власника інформації здійснюється в судовому порядку відповідно до законодавства України. Прикладами такої інформації, що підлягає пасивному захисту, є винаходи, корисні моделі, промислові зразки, торгові марки, фірмові назви, музика, драматургія, аудіовізуальні матеріали, література, різноманітні письмові результати, комп'ютерні програми, лекції тощо.

Під активним захистом комерційної таємниці розуміється, що власник встановлює певний спосіб доступу (наприклад, обмеження персоналу вузьким колом інформації, використання несанкціонованих копійованих носіїв тощо). Щоб зменшити можливість несанкціонованого використання. Таким чином, можна захистити таку інформацію, як «запатентована технологія», тобто інформація технічного характеру – закономірності, методи, результати різних досліджень, методи управління тощо.

Компанії зазвичай володіють інформацією, що належить до прав інтелектуальної власності, та загальнодоступною інформацією, тому керівникам слід поєднувати ці два методи захисту інформації.

За результатами дослідження можна зробити наступні висновки:

– комерційна таємниця має подвійну природу: з одного боку, це спосіб захистити конкурентоспроможність компанії від недобросовісних конкурентів, з іншого – призводить до нестачі інформації в економіці та веде до невизначеності ринку.

– невизначеність є нормою в ринковому середовищі, а комерційна таємниця є невід'ємною частиною успішної діяльності бізнесу.

– комерційна таємниця включає результати інтелектуальної діяльності (наприклад, винаходи, методи роботи, ноу-хау тощо) та об'єкти, які не містять ознак інтелектуальної власності (наприклад, списки постачальників і замовників, відомості про заробітну плату співробітників тощо).

– існує багато способів втратити комерційну таємницю, найпоширенішими є такі: конфіденційна інформація втрачається через халатне ставлення співробітників компанії, необхідно перевірити вимоги національних установ компанії (наприклад, АМК в Україні); у різних дослідженнях (зовнішні, бенчмаркингові дослідженнях тощо), методах недобросовісної конкуренції (наприклад, промислове шпигунство).

– компанія розрізняє два способи захисту комерційної таємниці

o пасивний і активний, які необхідно поєднувати для успішної діяльності компанії.

2 АНАЛІЗ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ ТА ОРГАНІЗАЦІЇ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ТОВ «СТЕМ»

2.1 Характеристика діяльності підприємства

Товариство з обмеженою відповідальністю «Стем» (ТОВ "Стем") займається виробництвом металопластикових конструкцій.

Організаційно-правова форма – товариство з обмеженою відповідальністю. ТОВ «Стем» діє відповідно до статутних договорів та положень.

Метою організації є отримання прибутку на користь учасників і співробітників, а також задоволення потреб населення в частині надання послуг і збуту.

Місія підприємства:

– задовольнити потреби клієнтів;

– збільшення виробництва та продажів;

– розширити ринок;

– ринкова вартість компанії значно зросла;

– посилення та підвищення конкурентоспроможності;

– прибуток.

Методами реалізації завдань є: підвищення ефективності фінансово-господарської діяльності підприємства; забезпечення високої якості продукції; забезпечення зростання виробництва та збуту; ефективна організаційно-функціональна структура та кваліфіковані працівники; висока технологічність виробництва та достатня оснащеність інформаційними технологіями.

Завдання діяльності ТОВ «Стем»:

– донести конкретні продукти до споживачів;

– дослідження споживчого попиту на товари;

– формування товарної сфери;

– реклама (розробка маркетингу);

– прийом замовлень на нерозпродажні товари;

– допомога клієнтам у виборі продукції та розробці дизайну для конкретних видів товарів.

Організаційна структура управління підприємством показана на рис. 2.1.

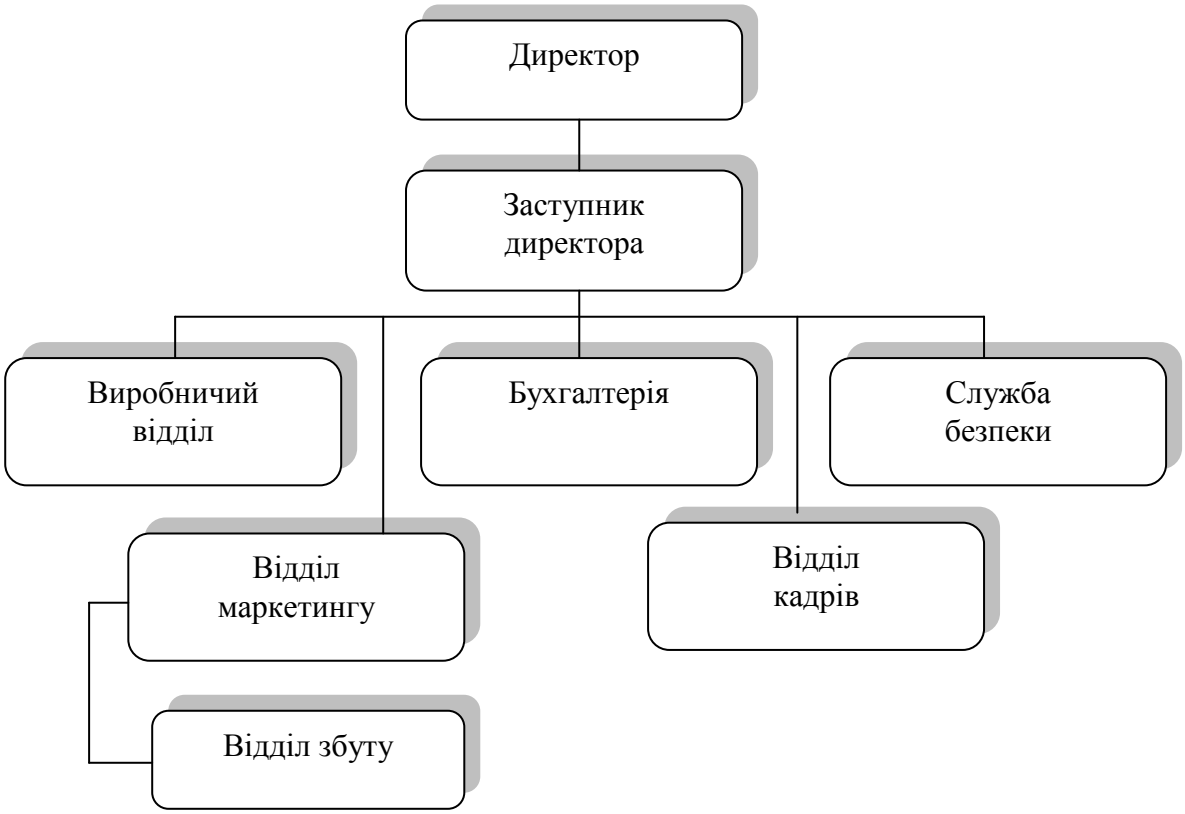

Рисунок 2.1 – Організаційна структура ТОВ «Стем»

Управління підприємством здійснюють директори, функції яких: здійснювати поточне керівництво, діяти від імені підприємства, представляти інтереси підприємства, видавати накази та розпорядження, визначати структуру управління, приймати на роботу та звільняти працівників, та відкрити поточні рахунки.

Заступники директора виконують свою роботу в межах покладених на них обов’язків і несуть повну відповідальність за своїх підлеглих.

До функцій бухгалтера входить ведення бухгалтерського обліку фінансово-господарської діяльності підприємства, підготовка річної та квартальної звітності, розрахунки з постачальниками та споживачами продукції, збір та аналіз оподаткування підприємства, операційних та бухгалтерських даних. Основне завдання бухгалтера – сформувати повну та достовірну інформацію про господарський процес та фінансові результати ТОВ «Стем», необхідну для функціонування та управління; забезпечити контроль наявності та руху майна та ресурсів; а також своєчасно сприяють негативним явищам фінансово-господарської діяльності.

Департамент маркетингу проводить комплексні дослідження кон'юнктури ринку. Основним завданням відділу маркетингу є формулювання ринкової стратегії та поведінки компанії з урахуванням її цілей, фінансових і технічних можливостей. У фокусі діяльності відділу маркетингу є: пошук і залучення нових клієнтів; розробка планів стимулювання; збір та обробка даних про діяльність різних відділів компанії; представлення агентів на виставках; аналіз та дослідження ринку; дослідження кон’юнктури; підготовка товару. прогнози попиту (також з урахуванням сезонності); розробляти маркетингові цілі та плани, виходячи з технічних і фінансових ресурсів компанії, організовувати та проводити рекламні кампанії; розглядати претензії клієнтів і партнерів, визначати їх інтереси та запити.

Відділ кадрів відповідає за утримання кваліфікованих працівників та набір працівників. Його функції: укомплектування виробничих планів (прийняття, розстановка, звільнення); ведення кадрової справи; аналіз плинності працівників і трудової дисципліни; складання наказів по особовому складу; удосконалення організації та структури управління; розробка штатного розпису та внесення змін на основі затвердженої

структури; систематичний нагляд за чисельністю працівників; контроль за виконанням законодавства про працю в частині оплати праці та нормування; аналіз роботи та умов праці; планування та прогнозування персоналу; положення про заробітну плату; адаптація персоналу; підвищення кваліфікації на основі оцінки праці; переміщення та звільнення працівників.

Основним призначенням служб безпеки є забезпечення безпеки підприємств та захист інформації та відомостей, що становлять комерційну таємницю. До функцій служб охорони належать: забезпечення охорони будівель, місць, обладнання, продукції та робочих технічних засобів, забезпечення безпеки під час усіх заходів (переговорів, зустрічей); запобігання несанкціонованому доступу та доступу до інформації, що становить комерційну таємницю; організовувати та забезпечувати системи доступу; співпрацювати з іншими підрозділами та підрозділами щодо формулювання та впровадження заходів щодо забезпечення обробки та організації документів, що містять відомості, що становлять комерційну таємницю, у всіх видах роботи. А також здійснювати нагляд за дотриманням вимог Директиви про захист комерційної таємниці.

Виробничий відділ займається виготовленням металопластикових конструкцій. Відділ збуту виконує замовлення, постачає та надає послуги з доставки продукції.

У повсякденній роботі ТОВ «Стем» керуються принципом забезпечення найвищої якості. З цією метою компанія підтримує партнерські відносини та співпрацю з провідними світовими та українськими компаніями, щоб максимально задовольнити потреби клієнтів та отримати конкурентну перевагу перед іншими компаніями на вітчизняному ринку металопластикових вікон.

У сучасних економічних умовах України ТОВ «Стем» продовжує ефективно працювати, шукає нові перспективні продукти та реорганізується

відповідно до сучасних умов. Щорічне зростання прибутку (вдвічі) свідчить про позитивну динаміку в суспільстві.

Показники, що характеризують фінансові результати діяльності підприємства, наведені у таблиці 2.1.

Таблиця 2.1 – Показники, що характеризують фінансові результати діяльності ТОВ «Стем» за 2019-2020 рр.

Показник	Фактичне значення показника		Відхилення	
	2019 р.	2020 р.	абсол. (+; -)	відносне, %
1. Чистий дохід від реалізації продукції, тис. грн.	138454,4	154127,8	15673,4	11,3
2. Собівартість реалізованої продукції, тис. грн.	119486,5	131298,3	11811,8	9,9
3. Чистий прибуток, тис. грн.	6342,6	8910,4	2567,8	40,5
4. Середньооблікова чисельність працівників, ос.	240	263	23	9,6
5. Продуктивність праці, тис. грн. /ос.	576,9	679,8	102,9	17,8
6. Рентабельність продажів, % (ряд.3/ряд.1)	4,6	5,8	1,2	-

Чистий дохід від продажів у 2020 році зріс на 11,3%, досягнувши 1541,2278 тис. грн.

Вартість виробництва в 2020 році склала 131 298 300 тис. грн., що на 9,9% більше, ніж у попередньому році.

Витрати підприємств за економічними факторами наведені в таблиці 2.2.

Таблиця 2.2 – Операційні витрати ТОВ «Стем» за економічними елементами

Показник	Фактичне значення показника		Відхилення	
	2019 р.	2020 р.	абсол. (+; -)	відносне, %
1. Матеріальні витрати, тис. грн.	80779,5	96684,0	15904,5	19,7
2. Витрати на оплату праці, тис. грн.	7488,7	10087,6	2598,9	34,7
3. Відрахування на соціальні заходи, тис. грн.	2657,5	3500,2	842,7	31,7
4. Амортизація, тис. грн.	3002,5	3525,6	523,1	17,4
5. Інші витрати, тис. грн.	3694,4	4101,5	407,1	11,0
Усього	97622,6	117898,9	20276,3	20,8

Сума операційних витрат на підприємстві зросла у 2020 р. на 20,8 % і склала 117898,9 тис. грн.

Структура витрат на підприємстві у динаміці наведена на рис. 2.2.

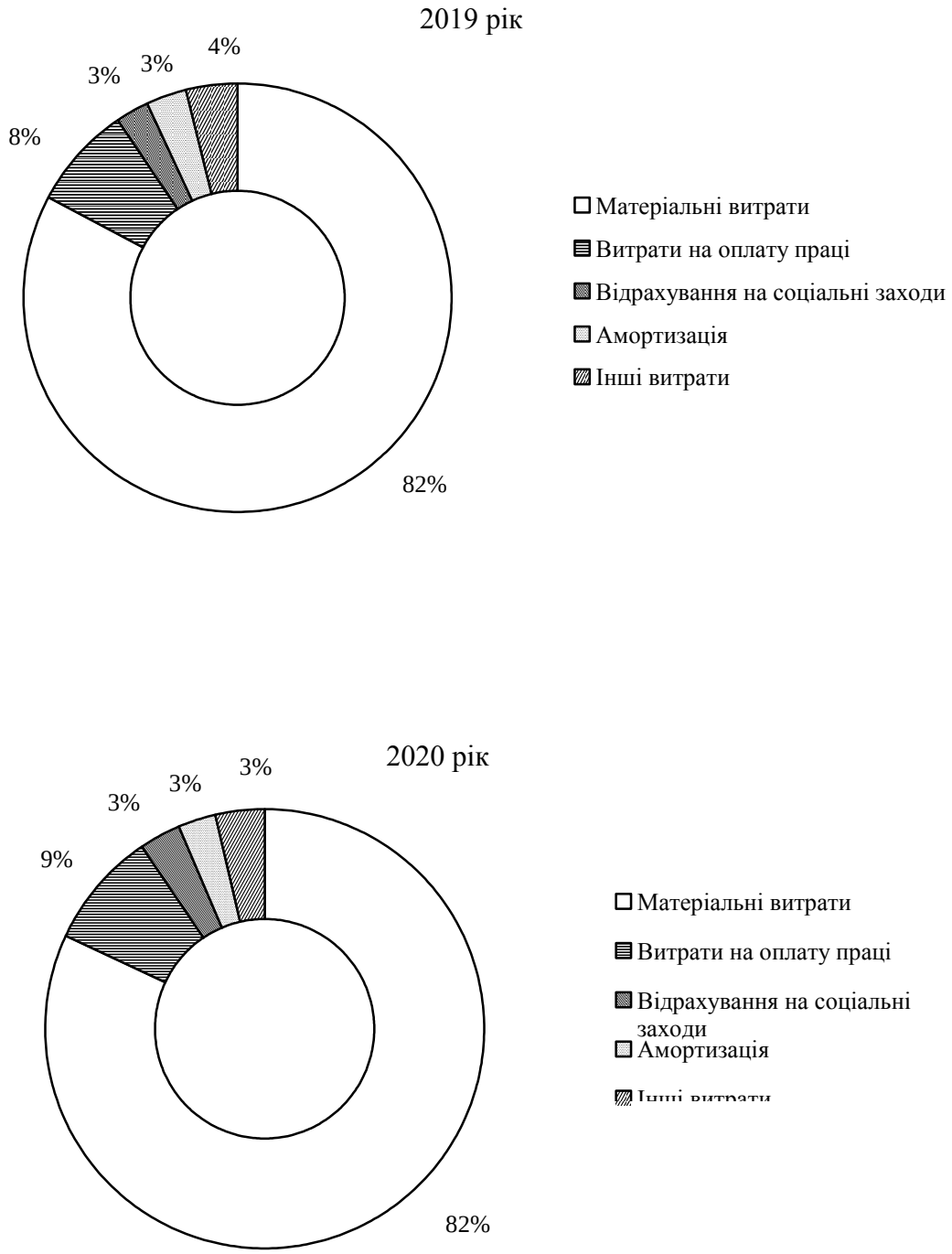

Рисунок 2.2 – Структура витрат за економічними елементами на ТОВ «Стем»

Серед видатків області у 2020 році найбільшу частку становили матеріальні витрати – 82%.

Графічно динаміка витрат ТОВ «Стем» наведена на рис. 2.3.

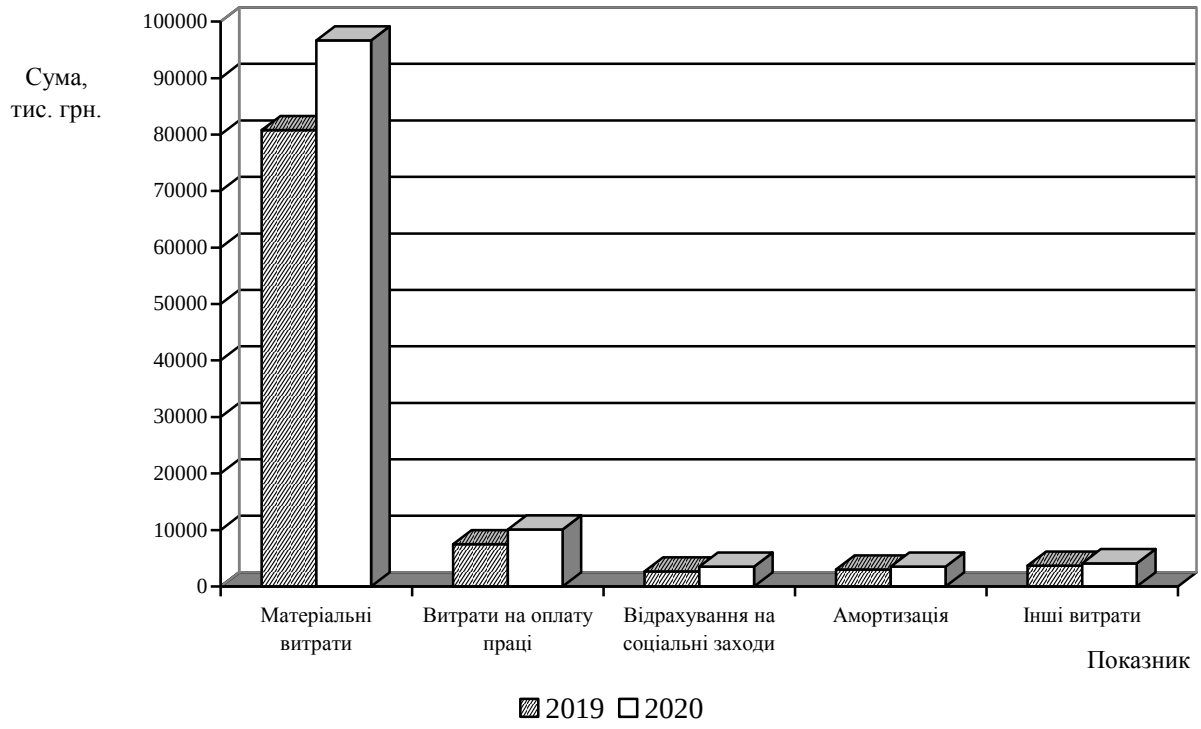

Рисунок 2.3 – Динаміка витрат на ТОВ «Стем» за 2019-2020 рр.

Чистий прибуток у 2020 році зріс на 2,5678 тис. грн., досягнувши 40,5%.

У 2020 році середньооблікова чисельність працівників зросла на 9,6%, що склало 263 осіб.

У 2020 році продуктивність праці підприємств зросла на 17,8 % і досягла 679,8 тис. грн./особу. Це свідчить про підвищення ефективності використання трудових ресурсів підприємства.

Рентабельність прибутку від продажів зросла на 1,2%. Це свідчить про те, що ефективність компанії підвищилася за період аналізу.

Динаміка основних показників, що характеризують фінансові результати діяльності ТОВ «Стем» за 2019-2020 рр., наведена на рис. 2.4.

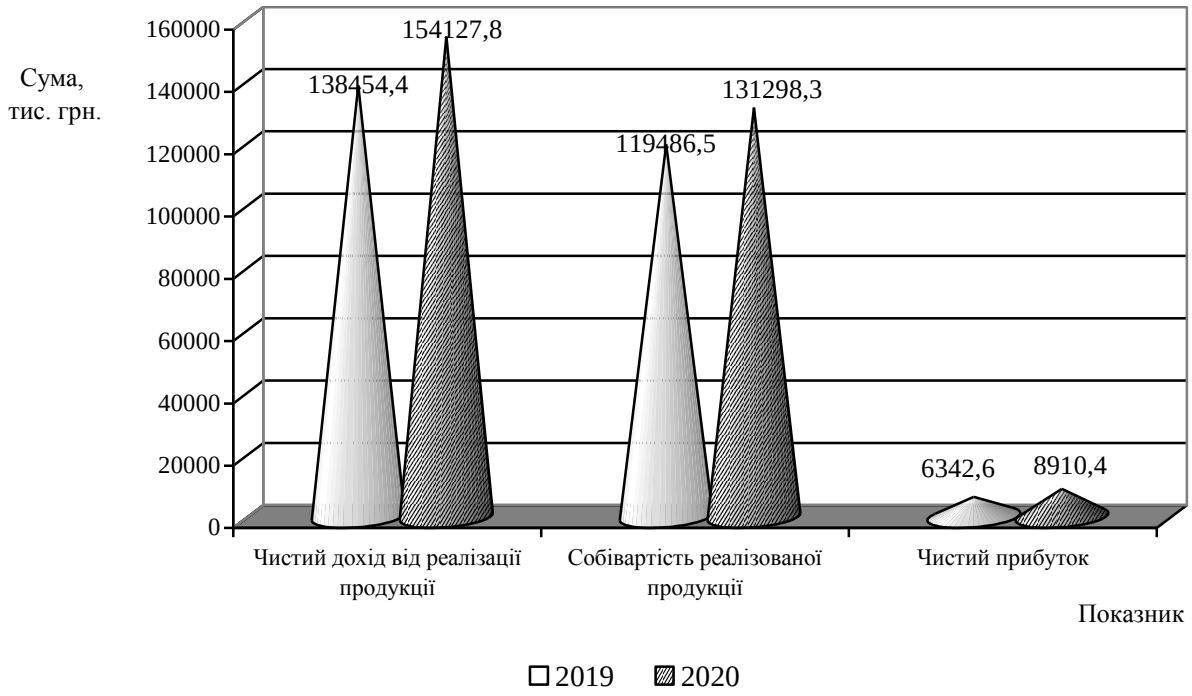

Рисунок 2.4 – Динаміка основних показників, що характеризують фінансові результати діяльності ТОВ «Стем»

На основі проведеного дослідження можна зробити висновки про позитивну динаміку основних показників діяльності ТОВ «Стем» у 2019-2020 роках.

2.2 Характеристика організації захисту комерційної таємниці на підприємстві

Служби безпеки підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційних компонентів економічної безпеки, зокрема [47]:

– збирати всі види інформації, пов'язані з діяльністю комерційних структур (інформація про всі види ринків; інформація, що описує політичні

події та макроекономічні тенденції розвитку світової та національної економіки; корисна науково-технічна інформація);

– аналізувати отриману інформацію та відповідати загальновизнаним принципам (систематизація, безперервність прийому, комплексна характеристика процесу аналізу) та методам організації роботи (локалізація під конкретні питання, загальна компанія);

– прогнозувати тенденцію розвитку технологічних, економічних та політичних процесів, пов’язаних з певною сферою бізнесу (діяльності) на підприємстві (організації), країні та світі, а також показники, яких має досягти суб’єкт (наприклад, фінансові прогнози, об'єкти прогнозу виробничо-технологічного розвитку);

– оцінити рівень економічної безпеки всіх компонентів та сформулювати рекомендації щодо підвищення реального рівня економічної безпеки окремих суб'єктів господарювання в цілому;

– розвиток інших видів діяльності інформаційної складової економічної безпеки (формування хорошого іміджу компанії, захист конфіденційної інформації).

Підприємства (організації) продовжують отримувати інформаційні потоки, і ці інформаційні потоки формуються (з'являються) з різних джерел. При цьому розрізняють:

– розголошення офіційної інформації;

– можлива неконфіденційна інформація, отримана шляхом неформальних контактів між співробітниками компанії та такими носіями інформації;

– отриманий несанкціонований доступ до конфіденційної інформації.

Розробка інформаційних компонентів економічної безпеки та оперативне впровадження захисних заходів досягаються шляхом послідовного виконання робіт, а саме:

– збирати різну необхідну інформацію через офіційні контакти з різними публічними джерелами інформації, неформальні контакти із закритими носіями інформації, а також за допомогою спеціальних технічних засобів;

– опрацювати та систематизувати отриману інформацію, яка буде здійснена відповідними службами підприємства (організації) для подальшого поглибленого аналізу. З цією метою створені класифікації інформації та архівів, внутрішні бази та довідники;

– аналізувати отриману інформацію, включаючи використання різноманітних технічних засобів та методів аналізу для комплексної обробки отриманих даних. У процесі аналізу використовуються різні методи моделювання для прогнозування та розрахунку різних аспектів інформаційної діяльності та можливої поведінки бізнес-середовища;

– захист інформаційного середовища підприємств (організацій) традиційно включає: захист суб'єктів підприємницької діяльності від промислового шпигунства з боку конкурентів або інших юридичних і фізичних осіб; технічний захист приміщень, транспорту, зв'язку, переговорів та різноманітних документів, запобігання пов'язаним законам несанкціонованого доступу. до конфіденційної інформації юридичних і фізичних осіб, збирати інформацію про потенційних ініціаторів промислового шпигунства та вживати необхідних запобіжних заходів для припинення таких спроб;

– зовнішня інформаційна діяльність спрямована на створення гарного іміджу компанії (організації) в очах громадськості та протидії спробам поширення неправдивої інформації, що завдає шкоди репутації компанії.

Перш ніж починати будь-яке серйозне планування, необхідно з’ясувати особливості ситуації. Цей процес не такий простий, як просто підрахувати кількість галузевих секретів, які необхідно захистити. В ідеалі

найкраще проводити офіційне дослідження, яке включає дослідження, польові дослідження, аналіз та визначення ступеня ризику.

З усім ключовим управлінським персоналом слід провести бесіду, щоб визначити, як вони розуміють проблеми та проблеми, які можуть бути метою шпигунства. Слідство також має визначити оцінку можливості розкриття таємниці та ступінь загрози таких інцидентів після успішної реалізації. З'ясування рівня розуміння різних суб'єктів – це не самоціль, а лише відправна точка процесу планування.

Опитування покаже, чи мають деякі виконавці вузько бачення проблеми в цілому. Вони можуть досліджувати деякі очевидні сфери промислового шпигунства. Насправді, якщо відповідальний за відділ безпеки або консультант зовнішньої організації під його керівництвом не дає виконавцю почуття відповідальності за дослідження, воно може бути абсолютно незадовільним і спотвореним через індивідуальні особливості виконавця. Навіть генеральний директор може не в змозі чітко побачити ситуацію і повністю передбачити всі можливості шпигунства.

Наступним кроком у процесі підготовки планування є проведення перевірки на місці. Тому необхідно оглянути деякі важливі об'єкти та визначити рівень захисту:

– захист усіх навколишніх об'єктів, включаючи паркани, стіни, ворота, шлагбауми, захисне освітлення та захист;

– стоянки транспортних засобів, їх розташування, огорожі та освітлення;

– захист системи освітлення;

– система безпеки службових собак;

– спеціальна структура віконного покриття та встановлення захисних засобів;

– охоронні та патрульні служби, система внутрішнього телебачення, контроль відвідувачів;

– послідовність зберігання замків і ключів;

– засоби пожежної безпеки;

– визначення забороненої зони;

– використовувати сейфи, камери та інші засоби для безпечного зберігання;

– визначати можливість витоку конфіденційних матеріалів з різних підрозділів компанії, потенційних об'єктів промислового шпигунства та інших небезпек, які можуть бути використані шпигунами, диверсантами або терористами;

– контролювати роботу співробітників на ділянках, які можуть порушувати режим роботи (наприклад, фотопомножувач, поштові лічильники, рахунки-фактури та інші фінансові бланки підприємства, які можуть бути використані шахрайським шляхом тощо);

– зосередьтеся на вербуванні, просуванні та призначенні в райони, які можуть бути мішенню шпигунів;

– регулярні перевірки всіх аспектів секретної діяльності під контролем начальника відділу охорони, включаючи передачу радіорепортажів, спостереження за внутрішніми телемережами та іншими методами спостереження, підслуховування, таємні зв’язки з дротовими лініями зв’язку, використання інформаторів та секретних агентів, секретні справи та записи, розробка планів протипожежної безпеки та аварійних ситуацій, навчання персоналу зв'язку, охорона, наявність кадрових і технічних ресурсів у службах безпеки.

План регулювання повинен мати відповідь на питання: «Що нам робити і чому?». Аналіз сильних і слабких сторін, масштабів і тенденцій промислової шпигунської діяльності, а також прогнозування майбутніх сфер діяльності промислового шпигунства забезпечать основу для визначення загальних проблем і пріоритетів, визначення низки проблем і формулювання політики стратегічного планування та настанови.

Стратегічне планування намагається відповісти на питання: «Що ми можемо зробити і як?». Використовуючи інформацію про нормативне планування та результати аналізу проблем для розгляду та оцінки альтернативних рішень, ми можемо почати розробляти плани та плани дій за непередбачених обставин, а також розробляти керівні принципи оперативного планування.

В оперативному плані виникає питання: «Коли і що будемо робити?». Використовуючи вказівки зі стратегії та планування, пропонуючи доступні обмеження та одержуючи оперативну інформацію, ми можемо розробляти проекти, складати бюджети та приступати до розробки кадрових та організаційних планів.

Отже, після завершення дослідження, складання планів і прогнозів, розгляду альтернатив, і ми знаємо, що потрібно зробити, ми можемо висунути гіпотезу щодо визначення проблеми та вибору завдання на основі плану регулювання.

Наступним кроком є визначення того, що можна зробити, і стратегічне планування шляхом вибору цілей, визначення альтернативних дій і вибору найкращої альтернативи. Вибір цілей буде залежати від змісту проблеми, оскільки результатом комплексу цілей є розв'язання задачі. Вибір цілей повинен здійснюватися в рамках глобальних цілей організації та в межах її ресурсів.

Перш ніж продовжити, необхідно включити загальні цілі всього обсягу в конкретні завдання, враховуючи терміни та виконання. Ці завдання мають бути проблемними, здійсненними, бажаними та сприяти досягненню обраних цілей (завдань). Завдання повинно включати досягнення вимірюваної величини або ступеня прогресу за певний період часу. Якщо період часу становить один рік, то, оцінюючи хід робіт щомісяця або щоквартально, можна визначити, чи виконано поставлені на рік завдання.

Підсумовуючи, можна визначити основні етапи наступних цілей відбору.

– визначення альтернативних цілей. Оскільки проблема може бути пов’язана з досягненням кількох цілей, ми повинні визначити ті, які є прийнятними, здійсненними та здійсненними. Це пов’язано зі сферою того, що можна зробити, яка називається стратегічним плануванням;

– вибір альтернатив. Досягнення деяких альтернативних цілей може бути серйозно обмежено. Треба розглянути переваги та недоліки інших цілей і вибрати найбільш підходящу;

– планування на основі впровадження. Вибір може включати багато окремих програм або програм. На цьому етапі ми вирішуємо, що робити чи виконувати оперативний план;

– виконання плану слід оцінити негайно. Використано два методи оцінки. Оцінка прогресу роботи зазвичай пов’язана з поточними проектами і обмежується отриманням відповідей на наступні запитання: Чи виконуємо ми завдання, як було заплановано? Які плани реалізуються? Скільки часу це витратило, а скільки витратили ми?

Оцінка прогресу може проводитися для окремих осіб, груп або всього проекту. У процесі оцінки впливу роботи на виконання плану стає зрозумілим, чи забезпечить це реалізацію цілей і завдань. Оцінка має бути безперервною, щоб забезпечити зворотній зв’язок, і на основі аналізу цілей, завдань, планів і прогресу реалізації проекту можна внести корективи для оптимізації всього процесу того, що компанія може вжити для захисту своєї комерційної таємниці. надано державою Запевнити?

Закони Китаю, Німеччини та США під комерційною таємницею розуміють інформацію. Для останнього захист комерційної таємниці можливий лише тоді, коли власник вживає достатніх заходів для захисту своєї конфіденційної інформації. В іншому випадку суд може відмовити в

захисті людей, які недостатньо дбайливо ставляться до захисту своїх таємниць.

Рішення може ґрунтуватися на оцінці технічних засобів захисту інформації, а також на оцінці загальної політики компанії у сфері обміну інформацією з третіми сторонами. Повернемося до України, особливо Закону про інформацію, який надає компаніям повну незалежність у визначенні змісту їхньої конфіденційної інформації та визначенні їхніх прав доступу. Ми хотіли б рекомендувати нашим законодавцям дозволити компаніям приймати нормативні акти для захисту їхньої комерційної таємниці. Порушення трудових прав нормативно-правових актів та інших правових галузей.

Комплексна система економічної безпеки підприємства - це сукупність взаємопов'язаних заходів організації, що реалізується спеціальними установами, службами, підрозділами суб'єктів господарювання, призначена для захисту життєво важливих інтересів громадян, підприємств і країни від реальних або потенційних протиправних дій. суб’єкта або юридичної особи, що завдає великих економічних збитків та забезпечує стійкий розвиток підприємства в майбутньому.

Основні завдання комплексної системи економічної безпеки підприємства:

– забезпечити економічну ефективність, фінансову стійкість та фінансову незалежність реальної господарської діяльності підприємства;

– захищати працівників суб'єктів господарювання, їх капітал, майно, законні права та підприємницькі інтереси від протиправних посягань з боку конкурентів та злочинних угруповань;

– збирати та аналізувати інформацію, що цікавить для прийняття ефективних управлінських рішень щодо економічної та безпечної стратегії та тактики розвитку компанії;

– на основі ефективного менеджменту та маркетингу компанії забезпечити високу конкурентоспроможність продукції, товарів і послуг;

– збирати, аналізувати та оцінювати інформацію про партнерів, конкурентів, замовників, інших фізичних та юридичних осіб для вжиття превентивних заходів та запобігання реальним та можливим загрозам економічній безпеці;

– забезпечити збереження матеріальної цінності, коштів та інформації, що становлять підприємницьку, банківську та іншу охоронювану законом таємницю;

– організовувати навчання персоналу підприємства та контролювати дотримання ним відповідних вимог, норм і правил, спрямованих на забезпечення економічної безпеки;

– сформулювати інструкції щодо дозволу співробітникам компанії на опрацювання документів, що містять захищені законом комерційні, банківські та інші конфіденційні документи, та організувати ведення діловодства.

Корпоративна економічна безпека – це стан корпоративних ресурсів (коштів, персоналу, інформаційних технологій, техніки та обладнання тощо), що забезпечує їх найбільш ефективно використання для стабільної діяльності та динамічного науково-технічного та соціального розвитку, запобігання внутрішньому та зовнішньому негативу. впливи (загрози).

Кожен суб’єкт господарювання потребує постійного дотримання економічної безпеки, що визначається завданням забезпечення стабільності діяльності та досягнення основних цілей його діяльності.

Забезпечення загальної безпеки підприємства потребує створення спеціального підрозділу для впровадження захисних заходів-служб охорони. Поява служб безпеки зумовлена загостренням внутрішньої та зовнішньої ринкової конкуренції та поширенням промислового шпигунства. Створення служб безпеки відображає об'єктивні потреби бізнес-спільноти щодо зниження бізнес-ризиків та підвищення безпеки підприємницької діяльності. Як правило, ці служби керують колишніми співробітниками правоохоронних

органів або відставними співробітниками розвідки та контррозвідки. Значна частина працівників – це люди, які в минулому брали безпосередню участь у вирішенні питань безпеки громадських установ.

Служби безпеки підприємства створюються відповідно до розміру підприємства. Зазвичай такі сервіси в основному створюються на великих підприємствах. У деяких випадках, залежно від їхньої важливості, вони можуть створюватися на середніх підприємствах.

У всіх інших випадках безпеку середнім і малим підприємствам забезпечують місцеві правоохоронні органи або органи національної безпеки.

Основні функції, які виконує служба безпеки, можна виразити так:

– захищати виробничо-господарську діяльність, а також захищати інформацію, що належить до комерційної таємниці підприємства;

– організовувати правовий та інженерний захист комерційної таємниці;

– не допускати необґрунтованого прийняття та одержання інформації, що становить комерційну таємницю;

– організовувати спеціальне діловодство і не може отримати інформацію, що становить комерційну таємницю;

– визначати та знаходити канали, які можуть розкрити конфіденційну інформацію під час діяльності та в крайніх випадках;

– установити та організувати систему безпеки для всіх видів діяльності, за винятком зустрічей, переговорів та зустрічей в рамках ділового співробітництва між підприємством та іншими партнерами;

– забезпечувати охорону приміщень, обладнання, офісів, продукції та технічних засобів, необхідних для виробничої чи іншої діяльності;

– організовувати особисту безпеку керівників, керівників підприємств та експертів;

– оцінити маркетинг і незаконну поведінку конкурентів і зловмисників.

Перелік конкретних завдань і функцій залежить від типу об'єкта, його структури, деталей його діяльності і може мати інші функції і завдання. Для кожного об’єкта охорони вони визначаються індивідуально.

У нормативних документах, що визначають організацію служби корпоративної безпеки, визначено конкретні об'єкти, які підлягають захисту від потенційних загроз та незаконного привласнення. Основні об'єкти безпеки такі:

– керівники та службовці, які володіють інформацією, що становить комерційну таємницю;

– матеріальні активи та фінансові ресурси (будівлі, споруди, обладнання, транспорт, валюта, цінності, фінансові документи);

– обмеження доступу до інформаційних ресурсів;

– підприємство (організація) комп'ютеризовані методи та системи;

– технічні засоби та системи захисту та захисту матеріальних та інформаційних ресурсів.

Залежно від конкретної ситуації підприємства можуть бути й інші об'єкти охорони та охорони.

Служба безпеки підприємства завжди повинна бути готова до подолання кризової ситуації, яка може виникнути через конфлікт комерційних інтересів та інтересів злочинного світу.

Для управління безпекою підприємства буде створено кризову групу, до складу якої входять керівник підприємства, юристи, фінансисти, начальник відділу охорони. Метою антикризової команди є протидія зовнішнім загрозам для безпеки підприємства.

Загальні функції, які покладаються на служби корпоративної безпеки, показані на рис. 2.5.

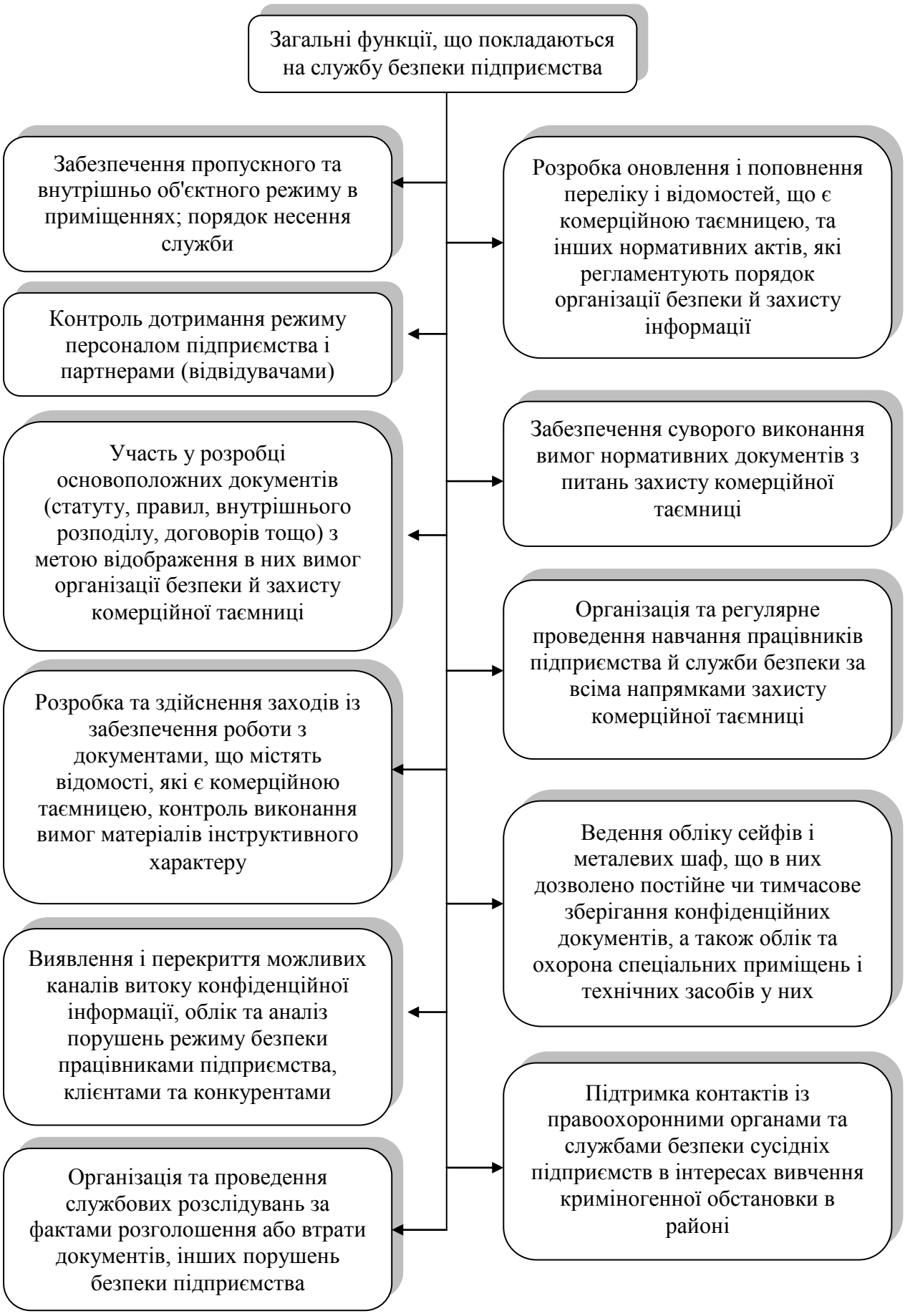

Рисунок 2.5 – Загальні функції, що покладаються на службу безпеки підприємства

Компанії можуть уточнювати та, за потреби, встановлювати власні специфічні функції персоналу охорони для повного забезпечення надійного захисту виробничих об’єктів.

2.3 Особливості організації захисту комерційної таємниці в системі економічної безпеки ТОВ «Стем»

Фактична робота із захисту конфіденційної ділової інформації включає кілька обов’язкових етапів.

Слід пам’ятати, що не має сенсу захищати добре відому інформацію законами про авторські права та патенти.

Запровадження конфіденційності не повинно суперечити фінансовому становищу та структурі управління підприємства. Економічні та організаційні помилки повинні бути внесені до захисту підприємства від торгівлі та стати основою конкретних планів Акт реалізації такого проекту, оскільки забезпечення конфіденційності інформації не повинно бути дорожчим за саму інформацію, а надмірна система, безсумнівно, знизить ефективність та результативність всього підприємства. Тому підприємству необхідно:

– визначити перелік конфіденційної інформації, яка незабаром стане об’ємом інформації, що становить комерційну таємницю. Їх кількість залежить від діяльності компанії та її масштабів, фінансових можливостей, зацікавленості конкурентів у її отриманні;

– установити процедури поводження з конфіденційною інформацією та контролювати дотримання цих правил, тобто обмежити доступ до конфіденційної інформації. Відповідальна особа затверджує порядок отримання та використання комерційної таємниці, а також перелік

працівників, яким дозволено ознайомлення з такою інформацією. Положення про комерційну таємницю підприємства повинні чітко впорядковувати угоди з контрагентами, які розкриваються комерційною таємницею, що вимагає окремого дозволу від партнерів;

– організувати систему обліку документів, позначених «комерційною таємницею», їх переміщення всередині та за межами підприємства, як доступ до співробітників його співробітників і ділових партнерів;

– організація реєстрації осіб, які отримали відомості, що становлять комерційну таємницю, і які нададуть або передадуть їм таку інформацію;

– включити до трудового договору з працівниками пункти, які передбачають відповідальність за розголошення комерційної таємниці у всій роботі компанії, а також визначити період, протягом якого ще існує зобов'язання щодо конфіденційності;

– включити пункт, який не розкриває економічні відносини керівництва як додаткове навантаження на існуючі обов'язки;

– використати печатку «Комерційна таємниця», щоб позначити документи та інші носії інформації із закритою інформацією, а також вказати повну назву та місцезнаходження компанії.

Видно, що поняття «комерційна таємниця» включає не лише секретну інформацію. Це передусім комплекс заходів, спрямованих на забезпечення корпоративної конфіденційності. Найважливішою умовою його реалізації буде правильно організований документообіг. На формулювання відповідних частин трудового договору, окремих договорів з працівниками, комерційних договорів та локальних нормативних актів слід приділяти найсерйознішу увагу, оскільки в разі неуповноваженості ця особа буде нести відповідальність і вимагати відшкодування завданих збитків.

Важливою частиною механізму захисту комерційної таємниці є налагодження робочого порядку з матеріальними носіями даного виду

інформації: кресленнями, дисками, стрічками тощо. При виборі зручної форми обліку конфіденційної інформації необхідно враховувати:

– відмітний знак (гриф) на документі не повинен перетинатися з грифом, який використовується при охороні державної таємниці;

– це зрозуміло лише співробітникам компанії і не може привернути увагу сторонніх;

– кількість кондорів має бути чітко визначена;

– робота підлеглих має бути організована за принципом «чистого столу». Суть полягає в тому, що працівники не повинні залишати жодних документів на своїх робочих місцях, коли вони відсутні. Вся інформація повинна надійно зберігатися в сейфі, металевій шафі або ящику столу.

Також у переліку необхідно вказати інформацію або конкретний період, коли інформація набула статусу комерційної таємниці.

Структурні підрозділи та співвиконавці повинні бути ознайомлені з їхніми неповними переліками, керуватися ними у своїй роботі та мати при собі печатки.

Перед підписанням будь-яких документів підрядники та керівники оцінюють, чи є якась інформація, що є частиною комерційної таємниці компанії.

Якщо у вас є така інформація на титульному аркуші першої сторінки в правому верхньому куті, потрібно поставити штамп. Наприклад, «комерційна таємниця». Список.

Ядром цієї робочої системи має бути зацікавленість виконавця у визначенні нових цілей захисту та визначення найкращого часу для зняття обмежень на поширення інформації.

При оприлюдненні раніше закритої інформації рекомендується більше уваги приділяти її практичній цінності та ексклюзивності, щоб викликати інтерес потенційних споживачів у країні та за кордоном до її використання.

Однак, якщо немає додаткової інформації від розробників, обсягу випущених даних має бути недостатньо для самореалізації.

Перш ніж керівництво підприємства візьме від працівників нерозголошення відомостей, що становлять комерційну таємницю, воно повинно виконати певні процедури: видати наказ про встановлення комерційної таємниці підприємству, затвердити перелік відомостей, що становлять комерційну таємницю, та зобов’язання затвердити форму нерозголошення відомостей, що становлять комерційну таємницю (протокол).

Незалежно від способу захисту комерційної таємниці, працівники повинні бути поінформовані під час виконання своїх обов’язків:

– процедури та процедури отримання статусу підприємця як комерційної таємниці через матеріали, документи та продукцію;

– відповідні правила отримання інформації про комерційну таємницю;

– обов'язки та обмеження, покладені на виконавців, які розпізнають конфіденційну інформацію (наприклад, ведення діловодства, облік, зберігання, копіювання, обробка інформації тощо);

– порядок прийому представників інших суб'єктів господарювання та передачі їм інформації;

– відповідальність за розголошення інформації, що становить комерційну таємницю підприємства, або порушення встановленого порядку роботи з нею.

У таблиці 2.3 наведено перелік відомостей, які можуть становити комерційну таємницю підприємств і обслуговуючих організацій [50].

Таблиця 2.3 – Перелік відомостей, що становлять комерційну таємницю [25-27]

Напрям	Перелік відомостей, що становлять комерційну таємницю
Управління	Відомості про перспективні методи управління виробництвом.
Виробництво	Організаційна структура підприємства; характер виробництва; організація праці на підприємстві; відомості про виробничі можливості підприємства; характеристика виробництва: дані про резерви сировини на підприємстві; відомості про фонди окремих товарів, у тому числі тих, що виділяються для поставок на експорт
Плани	Плани розвитку підприємства; відомості про плани підприємства з розширення виробництва; інвестиційні програми, техніко-економічні обґрунтування, плани інвестицій; планово-аналітичні матеріали за поточний період; обсяг майбутніх закупок за строками, асортиментом, цінами, країнами, фірмами; зведені відомості про ефективність експорту або імпорту товарів у цілому по зовнішньоекономічній діяльності
Фінанси	Відомості, що розкривають планові та фактичні показники фінансового плану; майновий стан; вартість основних засобів і товарних запасів; бюджет; обороти; банківські операції; відомості про фінансові операції; банківські зв’язки; специфіка міжнародних розрахунків із закордонними фірмами; планові та звітні дані по валютних операціях; стан банківських рахунків підприємства; рівень виручки; рівень доходів; боргові зобов’язання; стан кредиту (активи і пасиви); розміри й умови банківських та інших кредитів; розміри, джерела кредитів та умови за ними; рамки наданого підприємству кредиту; відомості про розміри запланованого кредитування; генеральна лінія і тактика у валютних та кредитних питаннях
Партнери	Характеристика клієнтури; дані представників, посередників, дилерів і партнерів; дані про покупців та споживачів (оптових і роздрібних); дані про постачальників; відомості про склад торгових та інших клієнтів, представників і посередників; негласні компаньйони товариств; комерційні зв’язки; місця закупки товарів; відомості щодо іноземних комерційних партнерах; зведення і характеристика підприємств-торгових партнерів (основні виробничі фонди, кредити, товарообіг); дані про клієнтів у торгівлі й рекламі; відомості про фінансовий стан, репутацію та інші дані, що характеризують ступінь надійності фірми або її представників
Контракти	Умови за контрактами, угодами – як укладеними, так і тими, що плануються (строки, обсяги, номенклатура, умови поставки); особливі умови контрактів (знижки, доплати, розстрочення платежів, опціони); умови платежів за контрактами (ціни, знижки, доплати, розстрочення платежів, опціони); особливі угоди й умови компенсаційних угод; відомості про виконання контрактів; відомості про номенклатуру та кількість товарів за взаємними зобов’язаннями, передбаченими угодами, протоколами, а також про товарообіг; відомості про авторські договори
Ціни	Відомості про методики розрахунків цін та принципи ціноутворення; структура цін; структура продажної калькуляції; калькуляція витрат виробництва; дані для калькуляції ціни.
Оплата праці	Умови укладень контрактів між адміністрацією підприємства і працівниками; відомості про оплату праці, преміальні, доплати і компенсації; відомості про авторські винагороди і гонорари

Засоби передачі та обробки та загальні заходи захисту інформації в мережі передбачають переважно використання апаратних, програмних та криптографічних засобів захисту. У свою чергу, апаратний захист використовується для вирішення наступних завдань:

– перешкоджати візуальному спостереженню та дистанційному прослуховуванню;

– усунення паразитного електромагнітного випромінювання та перешкод;

– виявлення засобів прослуховування та магнітного запису, які несанкціоновано встановлюються або переносяться на підприємства та банківські установи;

– захист інформації, що передається через зв'язок і знаходиться в системах автоматичної обробки даних.

За своїм призначенням апаратні засоби захисту поділяються на засоби виявлення та засоби запобігання несанкціонованому доступу. Слід зазначити, що універсального методу, який дозволяє виконувати всі функції, не існує, тому за типом несанкціонованого доступу для виконання кожної функції існують засоби пошуку та захисту. При цьому заходи по боротьбі з незаконним видаленням інформації за допомогою цих засобів є трудомісткими і дорогими, а також вимагають спеціальної підготовки.

Захист інформації від копіювання, виконуючи такі функції: визначення середовища, в якому може працювати програма; перевірка середовища, в якій виконується програма; реагування на запуски з несанкціонованого середовища; авторизація реєстрації копій; протидія вивченню системних алгоритмів.

Складність у визначенні того, яка інформація компанії захищена, полягає в тому, що та сама інформація буде вважатися конфіденційною в одному випадку і не вважатися конфіденційною в іншому. Кожен підприємець самостійно визначає склад відомостей, що становлять комерційну таємницю.

3 УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1 Напрями організаційного забезпечення захисту комерційної таємниці на підприємстві

Використання мікрофонів-парасольок, диктофонів-ручок чи камер-годинників для секретного збору даних може здатися вітчизняним лідерам ефектним елементом американського кіно, а не справжнім засобом конкуренції на внутрішньому ринку. Насправді, це лише деякі з різноманітних загроз інформаційної безпеки, які можуть спричинити знищення, видалення, модифікацію або блокування корпоративної інформації.

Конфіденційні дані та інформаційні процеси компанії повинні бути захищені від навмисно організованих і випадкових загроз. Сюди входять несанкціоновані особи або особи, які отримують доступ до інформації без дозволу, випадкові порушення роботи комп'ютера, лінії зв'язку, пожежі в будинках та стихійні лиха. У порівнянні з техногенними загрозами для людської діяльності, природні явища часто становлять меншу загрозу інформації.

Діяльність, організована для збору та використання конфіденційної інформації, може бути пов'язана не лише з розвідувальною поведінкою конкурентів, а й із бажанням співробітників заробляти всіма можливими способами, конфліктами в колективі, образами співробітників. помста. Згідно зі звітом аналітичної компанії, більшість навмисних атак на системи компанії здійснювали реальні співробітники та колишні співробітники.

Більше того, звичайний звільнений працівник навряд чи завдасть серйозних збитків компанії, а ось працівник з великою кількістю

повноважень та інформації може спричинити багато проблем. Це підтверджує справедливість наступного твердження: надійність будь-якого пароля визначається не його складністю, а непідкупністю шифрувальника.

Багато керівників вважають, що головна небезпека криється всередині компанії. Найпоширенішими інсайдерськими загрозами конфіденційності компанії вважаються хабарництво та вимагання співробітників компанії і лише потім видалення інформації з комп’ютерів, копіювання чи крадіжка файлів, прослуховування телефонних розмов та таємне відеоспостереження.

Витік або втрата інформації компанії зазвичай призводить до значних фінансових втрат, і керівники іноді не знають про це. Багатьом підприємствам досі важко визначити кількість інформаційних порушень своїх компаній. Деякі люди навіть не можуть бути впевнені, чи їхня інформація маніпулювалася злочинцями. Вітчизняні компанії усвідомлюють необхідність розуміння джерела загроз, порушників та поведінкових втрат і все більше уваги приділяють посиленню захисту інформаційних ресурсів. Все менше людей ігнорують це. До речі, вісім років тому термін «інформаційна безпека підприємства» використовувався лише невеликою групою експертів [51].

Для вирішення питань безпеки потрібен комплексний підхід. Створення ефективної та надійної системи безпеки передбачає поступове виконання ряду завдань, таких як формулювання стратегій безпеки, вибір методів захисту інформації, навчання співробітників, регулярні комп’ютерні аудити. Комплекс заходів щодо захисту інформації кожного бізнес-об'єкта залежить від масштабу, мети та характеру діяльності останнього. Експерти стверджують, що впровадження системи безпеки під час розробки інформаційної системи підприємства набагато дешевше, ніж у процесі.

Захист даних підприємства та контроль потоку інформації всередині підприємства мають здійснюватися на регулярній основі. Це питання вимагає постійної та зосередженої уваги. Зрештою, закон Мерфі ідеальний у сфері

інформаційної безпеки: якщо якась біда може статися, вона обов’язково станеться. Іронія полягає в тому, що багато компаній регулярно не аналізують безпеку своїх інформаційних систем, не усвідомлюючи, що безпека – це процес.

Створення системи корпоративного захисту.

Можливо зробити деякі загальні зауваження щодо створення системи корпоративного захисту. По-перше, фізичну безпеку організації слід розглядати в тісній взаємодії з інформацією. Однак ідентифікувати їх не варто, адже сьогодні можна вловити секрети компанії, не заходячи в приміщення за міцною стіною. Досить увійти в інформаційну систему, щоб отримати необхідні дані, відключити елементи мережі компанії або запобігти доступу до інформаційних ресурсів [52].

По-друге, захищати «все» нераціонально, і навряд чи дасть очікувані результати. У ньому має бути чітко визначено, яку інформацію слід захищати в першу чергу і кого слід захищати. Для цього вони проаналізували можливі методи навмисних і випадкових нападів, розробили модель потенційного порушника, яка врахувала його кваліфікацію, доступні засоби атаки, час дії та прогноз потенційних втрат.

По-третє, підхід «батог і пряник» особливо важливий у середовищах, де людський фактор може бути найбільшою загрозою. Головне, щоб організаційно-адміністративні заходи поєднувалися з психосоціальними заходами. Перший передбачає створення необхідної нормативно-правової бази шляхом формулювання організаційно-розпорядчих документів, на яких ґрунтується діяльність служб безпеки та відділів захисту інформації. Еталон виміру психосоціального характеру включає два основних аспекти: правильний підбір персоналу та використання матеріальних і моральних стимулів.

Західні експерти вважають, що збереження корпоративної таємниці залежить від відповідного підбору та стимулювання співробітників. Одним із

перших завдань досвідчених керівників є створення доброї соціально-психологічної атмосфери в організації, зниження плинності кадрів, формування «фірмового патріотизму». Не варто нехтувати запровадженням справедливої системи матеріальної винагороди, створенням можливостей кар'єрного росту та можливості участі персоналу у прийнятті рішень. Тільки при повному відношенні ролі роботи працівники можуть виконувати свої обов'язки найбільш ефективно.

Інформаційна безпека є одним із ключових принципів процвітання бізнесу. Ефективна система захисту дозволяє уникнути прямих і непрямих втрат, підтримує довіру до компанії і навіть підвищує її прибутковість. Навпаки, нестримний удар по інформаційним ресурсам послаблює організацію, адже давня хвороба пожирає організм людини. До речі, як всім відомо, лікарі підкреслюють, що це захворювання легше попередити, ніж лікувати.

Щоб захистити свій бізнес, компанія була змушена переконатися, що внутрішня інформація не витікає. Витоку даних можна запобігти, дотримуючись внутрішніх систем безпеки, формулюючи організаційні заходи, які забороняють співробітникам поширювати інформацію, і створюючи служби безпеки, які відстежують телефонні розмови, копіюють процеси та надсилають факси. Також просять допомогти у цьому системі відео-, аудіоконтролю та корпоративного контролю доступу, які ми розробляємо та впроваджуємо.

Деякі керівники все ще розглядають систему безпеки як економічно ефективну частину робочого процесу. Я помітив, що, навпаки, служба безпеки та всі її складові дозволяють зменшити втрати, а то й запобігти збиткам, і підвищити рівень всієї організації. Уникати збитків від недобросовісних співробітників або зовнішніх злочинців, особливо конкурентів, підвищити продуктивність праці за допомогою відеомоніторингу виробництва; за допомогою аналізу відеоінформації ми

можемо виявити недоліки в організації процесу, покращити організацію праці, зменшити збитки, підвищити рентабельність виробництва. Іншими словами, вкладаючи кошти в систему безпеки, менеджер вкладає кошти в розвиток свого бізнесу і отримує від цього прибуток.

Концепція безпеки формулюється разом із планом будівництва компанії, а всі комунікації, які забезпечує система безпеки, прокладаються в процесі будівництва. Так працює більшість новостворених організацій. Проте, як відомо, у Києві триває процес відновлення старих промислових підприємств, де таких систем або немає взагалі, або вони вже давно в аварійному стані. Їх модернізують і замінюють. Тому досвід показав, що монтаж сучасних систем безпеки здійснюється в процесі експлуатації та під час створення підприємства. Це залежить від його умов і наявності необхідних коштів [54].

Організація управління підприємством – складна і неоднорідна діяльність з управління підприємством. Темами такої діяльності є управлінський персонал і структура компанії, процедури і процедури прийняття управлінських рішень, системи комунікацій, у тому числі передача інформації від зовнішніх контактів до центру управління. Одним із вирішальних чинників у цьому питанні є правильна організація роботи з працівниками компанії, тобто кадрова політика. Стан психологічної атмосфери в колективі залежить від умов праці, створених керівником та його підлеглими.

Правильна організація підбору співробітників і розвиток їх зацікавленості в корпоративному успіху повинні бути спрямовані на мінімізацію плинності кадрів, водночас - на втрату корпоративного інтелектуального потенціалу і можливості розголошувати конфіденційну інформацію. Необхідно суворо дотримуватися правил поведінки та поводитися з інформацією, що становить комерційну таємницю компанії. З цією метою в трудовий договір (контракт), посадову інструкцію та правила

внутрішнього розпорядку підприємства мають бути включені пункти, які зобов'язують працівників неухильно дотримуватися правил поводження з конфіденційною інформацією, що є комерційною таємницею підприємства, та передбачати певну відповідальність за порушення. ці правила.

Вирішуючи питання соціального захисту працівників, їх медичне обслуговування, організовуючи кар'єрний розвиток, організовуючи розваги та дозвілля, керівники створюють у колективі середовище, яке мінімізує можливість усвідомлення працівниками шкоди для компанії. Власник, як суб'єкт внутрішнього контролю, повинен контролювати цілісність комерційної інформації, а також своєчасно виявляти та припиняти канали її розкриття.

Через організаційний хаос і недбалість, а також економічний та промисловий шпигунство інформація може бути втрачена. З метою захисту інформації, що становить комерційну таємницю, підприємство має вжити певних заходів: організувати відвідування підприємства сторонніх осіб. Правомірним є питання про запровадження корпоративної системи контролю відвідувачів. Немає необхідності наймати двірника на вході підприємства. Досить почати фіксувати реєстрацію відвідувачів і контакт з ними; з цього приводу рішення про посилення контролю внутрішнього та зовнішнього документообігу є дуже обґрунтованим, сформулювати внутрішні документи підприємства, що регламентують порядок роботи та ділову документацію, та обмеження доступу до конфіденційної інформації – це тимчасовий захід, і ви надасте його лише тим співробітникам, яким вона дійсно потрібна на роботі [55].

Конкретні обставини використання інформації, що зберігається в комп'ютері, визначають конкретні заходи щодо захисту такої інформації. Оскільки традиційні заходи інформаційної безпеки тут марні, програмне та апаратне забезпечення використовується для виключення можливості несанкціонованого доступу до комп'ютера та дослідження чи копії

інформації, що зберігається на ньому. Щодо зв’язку звітності з комерційною таємницею, то слід мати на увазі, що не всі види звітів є комерційною таємницею. Зокрема, закон вимагає розголошення фінансової звітності, тобто вона не може бути комерційною таємницею.

Це також стосується статистичних та податкових звітів. Однак дані внутрішнього звіту дуже деталізовані, тому їх можна використовувати лише внутрішньо. У зв'язку з цим внутрішні звіти часто є комерційною таємницею.

3.2 Розробка заходів щодо удосконалення організації захисту комерційної таємниці на ТОВ «Стем»

Для досягнення цілей і реалізації планів і проектів необхідно створити організацію. Розмір відділу безпеки компанії та обсяг її контррозвідувальної місії визначать, чи потрібно створити відділ чи іншу менш специфічну структуру. У будь-якому випадку найкраще зрозуміти принципи створення такої організації, яка не залежить від її розміру.

Організація служби безпеки та її контррозвідки передбачає такі дії [47]:

– розділити необхідну роботу на окремі завдання та види діяльності, визначивши повноваження та відповідальність;

– визначити функціональні обов'язки співробітників і зовнішнього обслуговуючого персоналу, встановити рівні та взаємовідносини;

– забезпечити роботу каналів зв'язку;

– відкоригувати співвідношення між різними робочими одиницями.

Зазвичай використовується організаційна схема. Забезпечте послідовність і послідовність за допомогою правил і процедур. Структурний план і документи специфікації відображають статус затвердження окремих завдань та ієрархічних підлеглих в організації.

При виборі організаційної структури, пов’язаної з контррозвідкою, необхідно враховувати фактор часу, оскільки охорону загалом і контррозвідку зокрема не можна планувати з 9:00 до 17:00 год. Необхідно враховувати інші специфічні функції. Експерти з аналізу інформації повинні бути готові приступити до роботи в міру необхідності, а експерти в певних галузях повинні працювати цілодобово. Організаційна структура повинна забезпечувати управління зверху вниз і зворотний зв'язок. Хоча контррозвідна діяльність значною мірою стане частиною загальних операцій з безпеки, для боротьби з промисловим шпигунством все ще потрібно створити спеціальний підрозділ або підрозділ.

Цей спецпідрозділ має бути невід’ємною частиною відділу охорони, але в певному сенсі він автономний. Він повинен мати власне керівництво, а керівництво підпорядковується керівництву відділу безпеки, через специфіку своїх обов'язків він повинен бути незалежним. Це передбачає, що начальник відділу контррозвідки безпосередньо і безпосередньо підпорядковується начальнику відділу безпеки.

Особливу увагу контррозвідувальний підрозділ має приділяти спеціальній підготовці своїх співробітників. Навряд чи у співробітників виникнуть дисциплінарні проблеми після проходження суворого процесу перевірки, але деякі вибрані люди можуть не бути повністю кваліфікованими для виконання цього завдання. Період навчання забезпечує сприятливі умови для адаптації оцінювачів до труднощів і особливостей служб безпеки. Навчально-екзаменаційний період дасть керівникам можливість позбутися тих, хто не виправдав очікувань.

Деякі навчальні програми поширюються на весь персонал контррозвідки, а інші навчальні програми стосуються лише професіоналів, які виконують «білі» та «чорні» функції. Усі члени команди повинні пройти навчання за базовим планом, розробленим для всього персоналу безпеки,

включно з протипожежною підготовкою. На цій основі має бути розроблений спеціальний план підготовки особового складу контррозвідки.

Члени цього підрозділу повинні розуміти природу розвідки, підривні фактори, загрози тероризму та диверсій, проходити навчання із засекречення та перевірки надійності документів, вживати заходів щодо запобігання та виявлення шпигунства, а також захисту підприємства від промислового шпигунства.

Співробітники, призначені для виконання «білих» функцій, пройдуть підготовку в галузі досліджень, аналізу та розвідки. Вони навчають використовувати комп'ютери для порівняння та узгодження даних, мати справу з тим, що маленька деталь у поєднанні з іншими деталями дасть додаткову інформацію. Вони повинні навчитися визначати прогалини в інформації, необхідній для емпіричної перевірки гіпотез. Вони зрозуміють, коли потрібно залучити колег, які виконують «чорні» функції.

Персонал, призначений для виконання «чорних» функцій, буде навчений мислити як шпигуни, підривники та терористи, щоб вони могли успішно виконувати контррозвідувальні місії. Вони вдосконалюють свої навички моніторингу та використання електронних пристроїв прослуховування, проведення таємних операцій, розслідування та допитів, ознайомлення з основами методів дослідження. Вони навчають мистецтву ідентифікувати загрози промислового шпигунства та типи персоналу, який може бути залучений. Вони вивчатимуть характеристики шпигунів, диверсантів та терористів з метою вжиття активних превентивних заходів.

Коротше кажучи, цей персонал буде навчений у дусі готовності захищати персонал та майно компанії, від управління та обладнання від диверсій до захисту комерційної таємниці від шпигунства. Ретельне дослідження ворога може забезпечити найкращий захист, щоб їхні знання в галузі промислового шпигунства не поступалися знанням їхніх злочинних супротивників.

Управління контррозвідкою – складне завдання. Керівники підрозділів безпеки, які ніколи не стикалися з проблемою організації, контролю та координації контррозвідувальних операцій, змушені будуть обробляти великі обсяги інформації за короткий проміжок часу. Але якщо він правильно вибере на посаду керівника контррозвідки роти, відсутність достатнього досвіду роботи керівника відділу охорони не стане перешкодою [8].

Керівник підрозділу розвідки має бути керівником, він взагалі не вирішує шаблонних завдань, що вимагає відмінних адміністраторських якостей. Менеджерам також важливо розуміти функцію та необхідність надсилання точної, своєчасної та важливої інформації тим, кому вона потрібна і кому дозволено доступ до неї. Він повинен володіти дослідницьким талантом і вміти керувати людьми, які мають можливість приймати самостійні рішення. Контррозвідка зазвичай займається досить складними питаннями, що вимагають тонких і швидких відповідей. В ідеалі керівник служби контррозвідки повинен бути в курсі останніх науково-технічних досягнень, які використовуються в промисловому шпигунстві. Звісно, не можна забувати, що сама по собі технологія не може вирішити всі проблеми вилучення розвідувальних даних, а для цього агенти-шпигуни повинні мати доступ до матеріалів, що цікавлять або людей, які володіють необхідною інформацією. Значна частина справді цінної інформації отримується шляхом підкупу посадових осіб, відповідальних за конфіденційність, або працівників, які мають доступ до конфіденційної інформації.

Діяльність контррозвідувального відділу компанії повинна бути узгоджена з вищим керівництвом і співробітниками організації. Підрозділ контррозвідки та відділ безпеки не можуть виконати всю роботу самостійно. Навіть маючи відмінні функції безпеки, внутрішні телевізійні мережі, замки та сигналізацію, повний контроль доступу та пильні охоронні та патрульні служби навколо будинку, успіх контррозвідки, як і будь-яка безпека,

залежить лише від людей. Начальник відділу охорони та начальник відділу контррозвідки повинні знайти спосіб розібратися з усіма в організації, від керівника виконавчого відомства до апарату. У цей час перед службами безпеки стоять нові завдання – це пов’язано з безпекою всіх співробітників і керівників усіх рівнів.

Якщо забезпечити хороший контроль інформаційної безпеки, координація буде ефективнішою. Цей контроль передбачає розробку управлінських процедур високого рівня для контролю всієї інформації для забезпечення ефективного управління. Цього можна досягти шляхом систематичного контролю всієї інформації, яка є життєво важливою для компанії. Участь різних відділів компанії надасть необхідні дані для вирішення проблем управління та прийняття рішень. Багато джерел даних включають листи, форми, звіти, результати досліджень, інструкції та рекомендації.

Якщо встановити контроль за поданням всієї вхідної інформації, ефективність контролю підвищиться.

Ефективність також залежить від контролю за порядком розповсюдження інформації, для якого мають бути встановлені нормативні правила: скільки документів надсилати та за якою адресою, які обмеження на доступ до цієї інформації (знак конфіденційності); з якою метою буде використана інформація.

Зберігання файлів є важливим аспектом безпеки даних. При цьому необхідно використовувати величезні можливості електронної обробки та зберігання даних. У цих випадках завжди потрібно пам’ятати про крихкість комп’ютерних запам’ятовуючих пристроїв і необхідність копіювання даних шляхом запису їх на жорсткий носій або стрічку. Також слід звернути увагу на носії інформації, такі як мікроплівка та мікроплівка.

Електронна система може записувати великі обсяги даних на дуже невеликій площі та забезпечувати миттєвий пошук. Електронні системи

зберігання також дозволяють авторизованим користувачам отримувати віддалений доступ до даних. Заходи безпеки дозволяють контролювати доступ, і люди, які мають доступ до інформації, потребують цього і мають на це право.

Для контролю даних потрібні стандарти зберігання та захисту інформації. Деякі дані можуть бути видалені через певний період часу; інша інформація повинна зберігатися протягом тривалого часу або не вказано конкретний період, якщо її природа представляє інтерес для архіву. Регулярне очищення файлів покращить ефективність системи.

Метою контролю даних є:

– своєчасно надавати точну та повну інформацію відповідним посадовим особам;

– ефективно обробляти, вводити пам'ять комп'ютера та поширювати інформацію;

– урахування стандарту «економічність» для забезпечення збереження даних;

– надати максимальний інформаційний сервіс для авторизованих користувачів.

Для того, щоб одночасно забезпечити ефективність та безпеку інформації перед шпигунськими агентами, необхідний хороший контроль інформації. Захист файлів конфіденційного відділу, особливо архівів і розвідки, має бути організований і жорстко контролюватися. Також потрібно звернути увагу на захист інформації всіх інших підрозділів компанії.

Незалежно від того, де зберігається критична інформація (таємний процес виробництва, обмежена фотокопія, комерційна таємниця компанії, опис майна та інші матеріали), всюди повинні бути забезпечені заходи безпеки та контроль за обліком конфіденційної інформації. Бухгалтерський контроль конфіденційної інформації є базовим елементом і важливою умовою безпеки протишпигунських інформаційних систем.

Планування та організація контррозвідки вимагає перевірених практик бюджетування. Так само, як облік конфіденційної інформації є основою безпеки інформаційної системи, наукове керівництво бюджетним процесом є інструментом боротьби зі шпигунством. В основному, бюджет - це план, виражений в доларах США. Вони є інструментом управління і можуть використовуватися як механізм контролю. Бюджет можна використовувати для оцінки прогресу, досягнутого у досягненні цілей з фінансової точки зору.

Оскільки успіх контррозвідки значною мірою залежить від загальних заходів безпеки, місія бюджету має бути ширшою, ніж задоволення одноразових фінансових потреб контррозвідки [38].

Бюджети проектів підкреслюють результати проекту та відображають загальний розподіл ресурсів, а не конкретні проекти, що фінансуються з бюджету. З іншого боку, детальний бюджет фокусується на звітності. Вони використовують цифрові індикатори для кожного проекту, щоб забезпечити фінансовий контроль. Більшість процвітаючих урядів та установ зараз використовують комбінацію планування та бюджетів проектів.

Відділ управління службою безпеки може поєднати переглянутий бюджет проекту з бюджетом проекту. Однак є сумнівним, чи доцільно використовувати оновлений бюджет типу проекту для переліку вимог до розвідки та контррозвідки.

Більшість державних розвідувальних агенцій використовують гнучкі бюджети планування без тягаря вимог по пунктах. Розумно використовувати подібні методи для підготовки бюджетів для промисловості та контррозвідки.

Дії приватного сектору можуть бути більш таємними, ніж дії державного сектору, оскільки про них не потрібно повідомляти громадськість і не привертатиме пильної уваги з боку ЗМІ. Однак у приватних промислових компаніях бюджети контррозвідки мають бути розроблені для забезпечення ресурсами на випадок надзвичайних ситуацій.

Тому його не слід перевантажувати індивідуальними вимогами. Бюджет планування повинен оцінювати загальні витрати, пов’язані з певним завданням, а не окремою статтею витрат.

Весь процес складання бюджету вимагає ретельного попереднього планування та постійного зворотного зв’язку та інформації з усіх відповідних джерел. Бюджет має бути оцінений, переглянутий і підзвітний. Ефективність цих процесів можна підвищити за допомогою комп’ютеризації. Необхідно оцінити прогрес і вплив. Оцінка ходу виконання виявляє якісні та кількісні показники рівня вирішення проблем, досягнутих для виконання плану.

Оцінка впливу використовує призму цілей і завдань для визначення успіху плану. Ще раз наголошуємо, що ці бюджетні аспекти будуть відповідати загальним заходам управління компанією у сфері безпеки.

Може виникнути питання: наскільки доцільним є бюджетний контроль, пов’язаний з розвідувальними та контррозвідувальними операціями. Це може бути одним із найважливіших управлінських питань для керівника відділу безпеки, який сформував у компанії контррозвідувальний відділ. Так само, як загальний бюджет потрібно планувати заздалегідь, бюджет контррозвідки вимагає більше зусиль, щоб спробувати спрогнозувати потреби в ресурсах.

Подібно до того, як загальний бюджет повинен контролюватися, і він сам по собі є інструментом контролю, так і бюджет контррозвідки також має контролюватися, і він сам по собі є інструментом контролю. Цілі схожі, але способи їх досягнення можуть бути різними.

Це вимагає високопрофесійного складання бюджету та найсуворішого контролю. Якщо бюджет буде занадто конкретним, гнучкість буде принесена в жертву, а якщо бюджет містить занадто багато змінних, ми втратимо контроль. Очевидно, що найкращим методом є використання бюджетів програмного типу для бюджетів контррозвідки для боротьби з промисловим шпигунством, а потім проведення ретельного внутрішнього аудиту та контролю.

Начальник відділу безпеки та його помічник з контррозвідки повинні знати, куди витрачається бюджет, і оцінювати операції, не ігноруючи критерії «економічність». Чи виконуємо ми ці плани, як було заплановано? Чи досягли вони бажаної мети? Якщо відповідь негативна, план слід переглянути. Однією з найбільших загроз для контррозвідки може бути небезпека бути звинуваченим у витрачанні великих сум грошей на підзвітність і неефективність [61-65].

Чесність людей, які працюють у компанії, настільки важлива для успіху діяльності компанії, що відділ безпеки повинен постійно перевіряти всіх співробітників. Досягнута з керівником відділу кадрів домовленість щодо поточного обміну інформацією має забезпечити зменшення загального витоку інформації, особливо тієї, що цікавить промислового шпигунства. Однією з особливих проблем у сфері службової злочинності (розголошення інформації, продаж таємниці чи участь у будь-якій іншій формі шпигунства на користь конкурентів, іноземних держав чи осіб, які займаються таємними промисловими операціями) є те, що порушники можуть мати рейтингові позиції в компанії.

Таку ситуацію можна віднести до злочинів «білих комірців» вищого керівництва. У цьому випадку керівник відділу безпеки повинен переконатися, що у нього є достатньо фактів, щоб перетворити гіпотезу на впевненість і довести, що ці сановники насправді є зрадниками його власної компанії. Поки його не заарештують, це може бути використано як урок для всіх співробітників компанії.

Для того, щоб начальник відділу охорони вживав заходів зі знанням ситуації, а начальник відділу контррозвідки уникав нашестя шпигунів, необхідно вести кадрові справи. Ці файли мають бути максимально конфіденційними та містити інформацію та розвідувальні дані рядового персоналу, отримані з різних джерел, включаючи офіційні державні установи. Одне з головних завдань начальника управління контррозвідки –

налагодити зв’язок з державними та приватними джерелами даних, що дозволить запобігти підкупу співробітників підприємства промисловими шпигунами.

У Сполучених Штатах важко отримати пряму допомогу від урядових організацій, поки не буде переконливо доведено військову або політичну загрозу національній безпеці. Тому служби безпеки переважно самодостатні й змушені проявляти ініціативу. Для складання ефективних документів оперативної розвідки розвідці більше, ніж іншим, потрібні новітні методи та хороші зв’язки.

Необхідно надавати велике значення персоналу та відповідним заходам для запобігання промислового шпигунства, як показано на рис. 3.1 [68]:

– перш ніж усі співробітники (нові та досвідчені) стикатимуться з комерційною таємницею та іншою конфіденційною інформацією, ретельно проінструктуйте їх, щоб вони розуміли конфіденційність інформації, яку вони мають, і усвідомлювали, що вони несуть відповідальність за те, як хтось розголошує таку інформацію;

– співробітники компанії підписують конфіденційні інформаційні конфіденційні документи;

– суворо контролювати документи, які визнані конфіденційними. Використовуйте захищену папку та передайте документи під розписку;

– контролювати копіювання таких документів та суворо обліковувати всі копії;

– вести поточний список толерантності з іменами осіб, які мають право та потребують знати інформацію;

– постійно аналізувати конфіденційні марки, щоб вчасно збільшити або зменшити їх відповідно до поточної ситуації;

– контрольований доступ до програмної інформації для представників ЗМІ та осіб, які не є співробітниками компанії. Заборонено отримувати будь-

які комерційні таємниці без дозволу керівництва компанії або юристів з авторських прав.

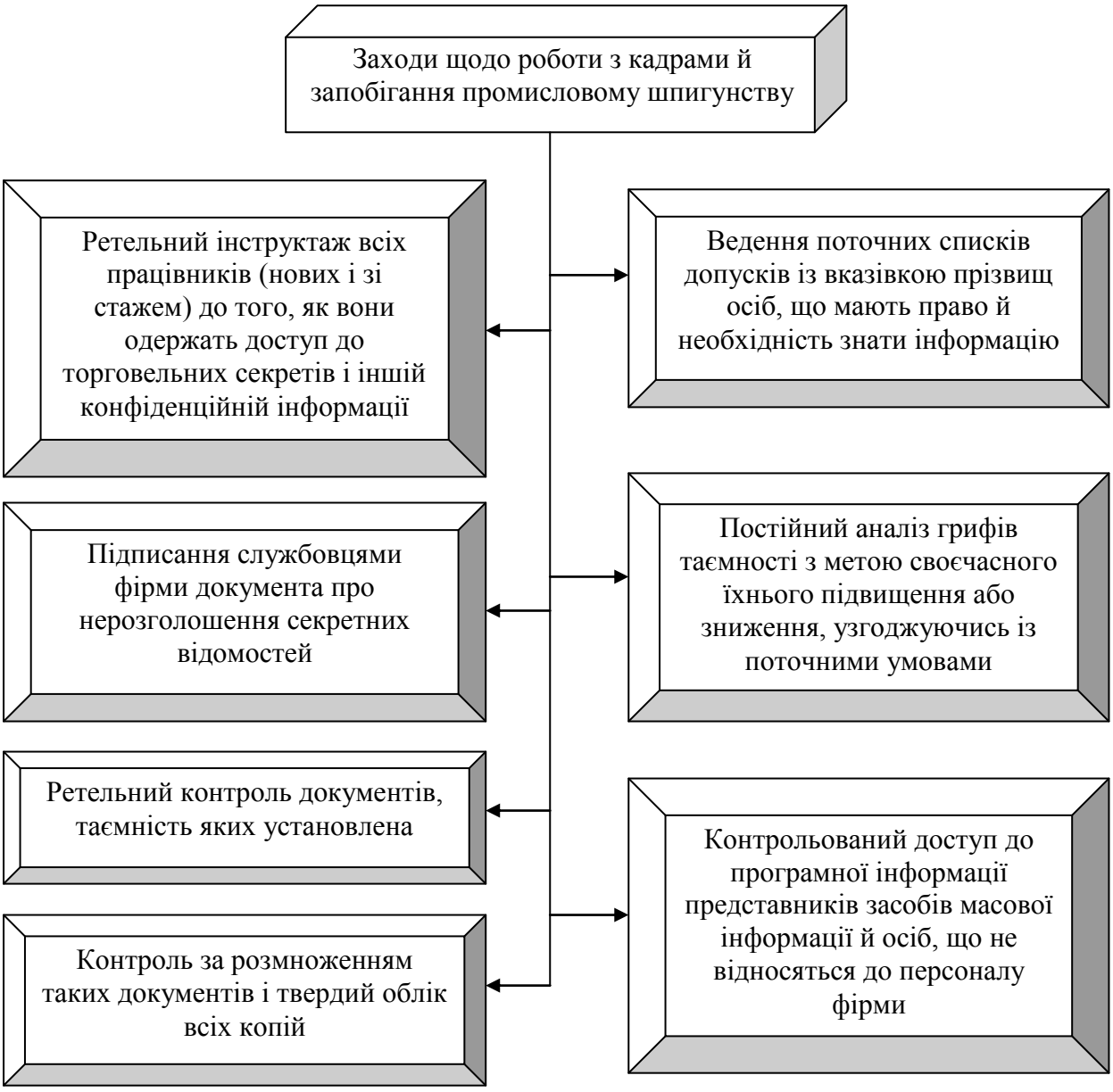

Рисунок 3.1 – Заходи щодо роботи з кадрами й запобігання промисловому шпигунству

Тому контррозвідна діяльність буде узгоджена з діяльністю відділу кадрів компанії та інших функціональних підрозділів. Все це безпосередньо впливає на успіх боротьби зі шпигунством, хоча деякі мають більший вплив.

Очевидно, особливу роль відіграє особа, яка відповідає за різноманітні проекти, пов’язані з юридичною службою та таємними операціями з майном компанії. Відділ зв’язків з громадськістю може бути помічником у діяльності компанії або перешкодою в залежності від розуміння проблеми та її внеску в боротьбу з промисловим шпигунством, диверсією та тероризмом.

Відділ зв’язків з громадськістю повинен мати можливість висловлювати думку про те, чи є об'єктом терористичної організації керівник адміністративного відділу чи саме підприємство. Прес-релізи не повинні повідомляти про діяльність компанії таким чином, щоб конфіденційна інформація була широко відома громадськості. Особливу увагу необхідно приділяти суворій секретності, посиленню захисту чиновників, примушенню ЗМІ та потенційних шпигунів і терористів шукати легші об’єкти для досягнення своїх цілей.

Майже всі компанії-конкуренти повинні вивчати ринок. Фактично, під виглядом дослідження ринку більшість операцій спрямовані на промислових шпигунів. У процесі дослідження ринку найкраще обмежити збір публічної інформації про конкурентів та їхню продукцію з точки зору власних інтересів безпеки компанії. Якщо компанія знає, що вона причетна до аналогічної протиправної діяльності, вона навряд чи зможе боротися з промисловим шпигунством. Відповідальний за відділ безпеки компанії зможе краще контролювати діяльність дослідників ринку та запобігати незаконній діяльності своєї компанії, чим успішніше він зможе боротися зі шпигунством ззовні.

Увесь світ є джерелом публічної інформації та великої кількості незаконно зібраних даних. До них належать [68]:

– аналізує продукцію конкурентів;

– відвідати виставку;

– порівняння рівнів продажів;

– проводити інтерв'ю з іншими конкурентами, нинішніми та колишніми співробітниками конкурентів, комерційних рекламних агентств та

іншими, знайомими з конкурентами та їх продуктами, щодо компаній-конкурентів та їх продукції;

– публікації, законодавчі слухання, рекламні оголошення та інші подібні матеріали.

Керівник відділу безпеки повинен усвідомлювати, що конкуренти не обмежуватимуть свою діяльність з маркетингових досліджень власною компанією. Сьогодні можна очікувати жорсткої конкуренції на ринку та прагнення до прибутку компанії та її працівників, особливо якщо акціями компанії володіє керівник відділу маркетингових досліджень. Через часту зміну керівного складу компанії важко очікувати лояльності до конкретної компанії, крім того, виникає питання, кому належать знання, якими володіють співробітники. Висока вартість і важливість досліджень визначають надзвичайно високу цінність комерційної таємниці. Уразливі місця в комп'ютерному сховищі, передачі інформації та програмуванні підвищують ризик промислового шпигунства.

Як щодо незаконної передачі інформації, отриманої дослідниками ринку? В основному від співробітників конкурентів або запрошених консультантів: надмірно активних торгових представників, наївних секретарок, безтурботних публіцистів, іноземних консультантів, сварливих співробітників, туристичних агенцій, дослідників, які враховують особисті інтереси, і, звичайно ж, шляхом підкупу чиновників або службовців.

Керівник відділу контррозвідки повинен знати, що дослідники ринку конкуруючих компаній можуть намагатися отримати інформацію нелегально, тому він повинен не тільки уважно стежити за спробами конкурентів викрасти фірмові секрети, а й уважно стежити за діяльністю співробітників компанії, щоб визначити міру. Сприяти успішній діяльності компаній-конкурентів.

3.3 Розробка проекту захисту комерційної таємниці на основі системного методу «OPSEC»

Сьогодні питання захисту власної інформації є одним із найактуальніших. У висококонкурентному світі компанії (бізнеси) змушені приділяти пильну увагу системі захисту комерційної таємниці (таємниці). Це пояснюється тим, що права інтелектуальної власності, такі як інформація, є товарами з великою комерційною цінністю для їх власників. Проте цінність інформації бачать не лише її власники, а й конкуренти. Тому фірма (підприємство) на будь-якому етапі своєї діяльності має приділяти пильну увагу системі захисту комерційної таємниці (таємниці), інакше це призведе до втрати доходу або банкрутства.

Комерційна таємниця – це недержавна таємниця, пов’язана з виробництвом, технологією, функціонуванням та фінансовою діяльністю підприємства Розголошення (передача, розголошення) інформації, яка може завдати шкоди інтересам підприємства [67].

Основою комерційної таємниці є власні цінні відомості, пов'язані з безпосередньою діяльністю підприємства. Ділова таємниця підприємства (комерційна назва) – це властивість, ефективне використання якої повинно приносити прибуток.

Інформація, що стосується рівня комерційної таємниці, є певною мірою товаром, ціна якого коливається від мільйонного прибутку до банкрутства. З цього можна зробити висновок, що нерозповсюдження та приховування інформації, яка є комерційною таємницею, від надійних конкурентів ускладнить їх поведінку та принесе підприємству економічну вигоду. Забезпечення збереження комерційної таємниці створює передумови для ефективних дій у конкретних сферах бізнесу та є перевагою в економічній конкуренції.

З цієї причини будь-яке підприємство має захищати комерційну таємницю як сукупність цінної інформації.

Захист інформації – це регулярне використання методів і технологій для прийняття рішень та здійснення заходів щодо систематичного забезпечення необхідного рівня захисту інформації. Ця мета досягається шляхом створення системи захисту інформації, яка являє собою сукупність методів і підходів до забезпечення захисту [67, 68].

Для ефективного захисту комерційної таємниці підприємств керівники та працівники служб безпеки підприємства повинні розробляти та реалізовувати проекти захисту комерційної таємниці.

Проект «Захист комерційної таємниці підприємства» – це унікальна та взаємопов’язана комплексна дія, спрямована на своєчасне виявлення та усунення причин та умов, які сприяють розголошенню комерційної таємниці в умовах обмежень якості, ресурсів, цілей та умов.

Для успішної реалізації проекту необхідно визначити [70]:

– що потрібно захищати, кого захищати, коли і якими засобами;

– хто організовує та забезпечує охорону;

– хто оцінює ефективність та достатність захисту;

– яка вартість захисту.

Системний підхід до вирішення цих проблем має бути представлений у вигляді чіткої та формальної методології «OPSEC» (Operation Security). Цей метод є циклічним, оскільки після кожного етапу потрібен «самоконтроль», щоб проаналізувати оптимальність вжитих і виконаних заходів.

Процес організації захисту інформації за методом «OPSES» здійснюється поетапно під час формулювання та реалізації проекту захисту.

Основні етапи методу «OPSES» організації процесу захисту інформації показано на рис. 3.2.

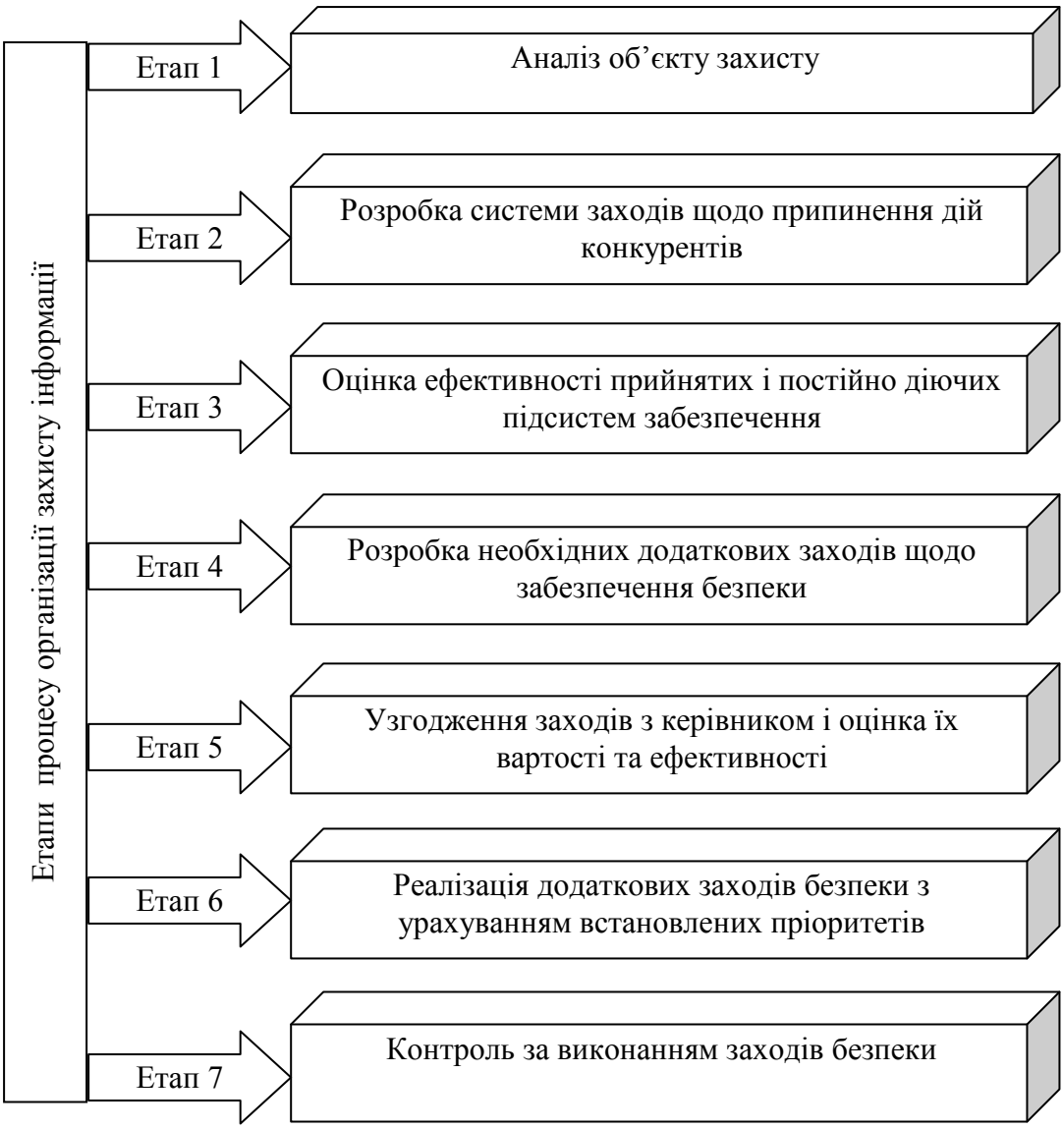

Рисунок 3.2 – Етапи процесу організації захисту інформації за методом «OPSEC»

Перший етап «Аналіз охоронюваних об’єктів» полягає у визначенні об’єктів, які потребують охорони. На цьому етапі потрібно встановити наступне:

– яку інформацію необхідно захистити;

– найважливіший елемент (ключ) захищеної інформації;

– життєвий цикл ключової інформації (час, необхідний учасникам для реалізації отриманої інформації);

– ключові елементи (показники) інформації, що відображають характер захищеної інформації;

– класифікувати показники за функціональними сферами діяльності підприємства (виробничо-технічні процеси, виробничо-логістичні системи, співробітники підприємства, фінанси, менеджмент тощо);

– визначити цінність комерційної таємниці.

Для цього використовується метод визначення цінності комерційної таємниці – перед розробкою системи інформаційної безпеки необхідно оцінити ступінь захисту, що залежить від економічних показників та ефективності. При цьому оцінка має бути достатньо об'єктивною, як технічно, так і економічно. Крім того, сучасні економічні стандарти мають перевагу над усіма іншими стандартами.

Сьогодні в якості нормативів економічної ефективності широко використовуються наступні стандарти: термін окупності, зниження витрат і скорочення витрат, які розраховуються на основі перших двох стандартів.

Термін окупності ($Т_о$) розраховується за формулою [70]:

$$T_o = \frac{C_к}{E_т - C_р}, \qquad (3.1)$$

де $С_к$ – одночасні капітальні витрати на момент встановлення системи;

$Е_т$ – позитивний ефект в одиницю часу, одержаний від впровадження системи захисту інформації;

$С_р$ – експлуатаційні витрати в одиницю часу.

Приведені витрати ($С_{пр}$) розраховуються за формулою [70]:

$$C_{пр} = C_к + O_н \cdot C_р, \qquad (3.2)$$

де $О_н$ – нормативний термін окупності;

З – повні витрати:

$$З = C_к + T_c \cdot C_p, \qquad (3.3)$$

де T_c – термін служби або передбачуваний термін використовування системи захисту інформації.

Окрім відмічених вище критеріїв, роблячи економічну оцінку системи, необхідно також враховувати витрати на неї і взаємодію між підсистемами, які входять до її складу.

Тому можна припустити, що повна вартість системи захисту інформації буде сумою вартостей складових її підсистем [70]:

$$C_n = C_o + \sum_{i=1}^{n} \frac{C_i}{(1+r)^i}, \qquad (3.4)$$

де C_o – інвестиції;

i – і-й період дії заходу (i=1,n);

C_i – грошові надходження у періоді і;

r – вартість капіталу.

На другому етапі запропонованої моделі:

– визначити, хто може бути зацікавлений у захищеній інформації;

– оцінити методи, якими користуються конкуренти для отримання цієї інформації, та можливе використання вразливостей існуючих систем безпеки компанії за певних обставин;

– розробляти систему заходів щодо запобігання діям конкурентів.

На третьому етапі аналізується ефективність визнаних і постійних підсистем безпеки (фізична безпека, безпека файлів, надійність персоналу, безпека ліній зв'язку, що використовуються для передачі конфіденційної інформації тощо).

Змоделювати заплановані операції та опишіть часову послідовність подій (або їх функціональні зв’язки), які повинні забезпечити безпеку. Для

кожної події запланованої операції визначаються показники, які можуть бути використані як відправна точка для визначення ключової інформації.

Визначити можливі конкретні джерела інформації, і їх аналіз може привести до визначення таких показників (статті новин, прес-релізи, телефонні розмови на незахищених каналах, недбале ставлення до проекту, зайва інформація, що передається під час переговорів, і стереотипи). , робота та процедури в повсякденному житті тощо).

На четвертому етапі на основі аналізу та досліджень, проведених на перших трьох етапах, визначаються необхідні додаткові заходи безпеки. При цьому «закриття» переліку додаткових захисних заходів, які виявили вразливі місця, супроводжується оцінкою витрат, пов’язаних із застосуванням кожного заходу. Порівнюючи очікуване зниження вразливості та майбутні витрати, можна оцінити економічну доцільність запропонованих заходів.

На п’ятому етапі керівники компанії, компанії та організації розглядають усі необхідні заходи безпеки та розраховують їх вартість та ефективність.

Шостий етап – етап впровадження додаткових заходів безпеки з урахуванням встановлених пріоритетів.

На сьомому етапі контролюється виконання заходів безпеки. Це перевіряє ефективність вжитих заходів та визначає вразливі місця, які ще не захищені або з’являються знову.

Впроваджені заходи досягли оптимального рівня, а його функції постійно контролюються.

Команда проекту відіграє важливу роль у розробці та реалізації проекту. Необхідно належним чином делегувати повноваження, розподіляти права, обов’язки та взаємовідносини всередині команди проекту.

З точки зору змісту, команда проекту – це група висококваліфікованих експертів, які володіють певними знаннями та навичками, необхідними для ефективного досягнення цілей проекту. Важливою особливістю команди

проекту є підприємницький характер її діяльності, спрямований на вирішення погано структурованих проблем та швидке реагування на вимоги навколишнього середовища та мінливі умови проекту. Форма та час існування команди незмінні. [73]

Матриця відповідальності проекту захисту ділової таємниці наведена в таблиці 3.1 [75].

Таблиця 3.1 – Матриця відповідальності

Задача	Відповідальний							
	Керівник фірми	Рада безпеки	Начальник суслу безпеки	Юрист	Відділ режиму і охорони	Спецвідділ захисту комерційної таємниці	Група інженерно-технічного захисту	Сектор забезпечення безпеки зовнішньої діяльності
Охорона будівель і приміщень			V		V			
Розробка переліку закритої інформації			V			V		
Організація інженерно-технічного захисту конфіденційної інформації							V	
Оцінка і прогноз роботи з партнерами і конкурентами								V
Інформаційно-аналітична робота								V
Охорона устаткування і ліній зв'язку					V			
Забезпечення режиму секретності документів і матеріалів			V			V		
Блокування несанкціонованого отримання інформації за допомогою технічних засобів							V	
Система норм, юридичний представник				V				
Використовування заходів державного і адміністративного примушення	V							
Підготовка і перепідготовка кадрів, атестація фахівців	V							
Контроль за станом і надійністю захисту закритих робіт	V		V					
Забезпечення режиму допуску			V			V		
Організація пропускного режиму					V			
Захист баз і банків комп'ютерних систем							V	
Розробка програмних засобів захисту			V				V	
Розслідування випадків порушення		V	V			V		
Розробка програми захисту			V					
Узгодження програми захисту		V						
Затвердження програми захисту	V							

Під час процесу розробки будь-якого проекту, через певні особливості проектної діяльності, ризики проекту будуть зустрічатися протягом усього життєвого циклу.

Ризик проекту – це сукупність ризиків, які загрожують реалізації інвестиційного проекту або знижують його ефективність (комерційний, економічний, бюджетний, соціальний, економічний тощо) [71, 72].

У таблиці 3.2 наведено класифікацію ризиків під час розробки проекту для захисту комерційної таємниці підприємства з урахуванням фази проекту.

Для ефективної реалізації проекту необхідно керувати ризиком.

Управління ризиками – сукупність управлінських дій і заходів, які впливають на суб'єктів господарювання, забезпечують максимально широке покриття ризиків, розумно визнають і доводять його вплив до максимально можливої межі, щоб зменшити можливість випадкових (неочікуваних) несприятливих подій і компенсувати його вплив і наслідки [72].

У розроблених на практиці основних принципах управління ризиками можна виділити наступні моменти [73, 74]:

– ви не можете ризикувати більше, ніж власний капітал, який він може собі дозволити;

– необхідно враховувати наслідки ризиків;

– не можна ризикувати, щоб бути малим.

Тільки за наявності на підприємстві нормативних документів (інструкцій) щодо захисту комерційної таємниці та з урахуванням необхідних вимог та умов підприємство може ефективно захищати комерційну таємницю.

Розробка та реалізація проекту захисту комерційної таємниці потребує певних витрат. Тому на етапі планування проекту необхідно враховувати цінність комерційної таємниці.

Таблиця 3.2 – Класифікація ризиків проекту захисту комерційної таємниці на підприємстві [65]

Фаза	Фактор ризику
Передінвестиційна	1. Визначення цілей, задач, результатів, (чітке формулювання, нечітке формулювання)
	2. Збір даних на підприємстві (інформація достовірна, інформація недостовірна)
	3. Наявність аналогічних продуктів, технологій, винаходів, у конкурентів (так, ні)
	4. Розробка концепції проекту (правильна, помилкова)
	5. Ефективність інвестицій (ефект є, ефекту немає)
	6. Ухвалення рішення щодо інвестування (витрати мінімальні, вигоди максимальні)
	7. Ухвалення рішень щодо включення тих або інших даних про діяльність підприємства в «Перелік відомостей, що становлять комерційну таємницю» (правильне, помилкове)
	8. Використовування додаткових критеріїв віднесення інформації в ранг комерційної таємниці (так, ні)
Інвестиційна	1. Платоспроможність фірми (стабільна, нестабільна)
	2. Зміна в технічному і робочому проектах (немає змін, істотні зміни)
	3. Зрив термінів (ні. ризик значний)
	4. Кваліфікація персоналу (висока, низька)
	5. Шахрайство, злом систем безпеки (так, ні)
	6. Підвищення цін на комплектуючі для системи безпеки (більше 5%, більше 100%)
	7. Підвищення витрат у зв'язку з несподіваними державними заходами податкового і митного регулювання (ні, ризик значний)
	8. Підвищення витрат на зарплату (більше 5%, більше 100%.)
	9. Удосконалення комп'ютерних інформаційних систем, технологій, програмного забезпечення (значні, незначні)
	10. Надійність персоналу (достатня, недостатня)
Експлуатаційна	1. Забезпеченість оборотними коштами (висока, низька)
	2. Поява нового продукту, технологій, «ноу-хау» та ін. (конкурентоспроможність висока, низька)
	3. Удосконалення продуктів, устаткування, технологій та ін. (ні, ризик значний)
	4. Шахрайство, злом систем безпеки (так, ні)
	5. Неплатоспроможність споживачів (незначний час. тривалий час)
	6. Надійність технології (достатня, недостатня)
	7. Надійність персоналу (достатня, недостатня)
	8. Рівень конкурентоспроможності (високий, низький)
	9. Підвищення витрат на зарплату (більше 5%, більше 100%)
	10. Недостатній рівень заробітної плати (зростання на кожен відсоток інфляції, зниження при зростанні інфляції)
	11. Відношення до проекту власті (позитивне, дуже негативне)

Команда проекту має велике значення для ефективної реалізації проекту. Процес формування команди необхідно розглядати як створення єдиної інтегрованої управлінської команди, здатної ефективно досягати цілей проекту. Командна робота персоналу дозволяє підвищити продуктивність управлінської роботи на 70-80%. Крім того, якщо немає ідентифікації та ефективного управління ризиками, ефективна реалізація проекту неможлива. Для цього компанія повинна мати кваліфікованих менеджерів з навичками оцінки ризиків. Оцінка ризику передбачає діагностику ризикової ситуації, сфери підприємницької діяльності та проведення якісного та кількісного аналізу ризику [75].

В організаційному плані ТОВ «Стем» рекомендується ввести в дію «Положення про захист інформації, що становить комерційну таємницю та конфіденційну інформацію».

Сферою використання запропонованої розробки є організація та управління фінансами підприємства та економічною безпекою.

Функціональне призначення – організація та юридична підтримка компаній щодо захисту комерційної таємниці.

Пропонованими користувачами можуть бути директор, заступник директора та відповідальний за служби безпеки підприємства.

Фактичними об’єктами застосування результатів дослідження можуть бути комерційні та некомерційні підприємства, посередницькі організації, фінансові установи, страхові компанії будь-якої форми власності та різного виду діяльності.

ВИСНОВКИ

У першому розділі роботи розглянуто теоретичні засади організації захисту комерційної таємниці на підприємстві.

Розкрито суть комерційної таємниці та одержання інформації про конкурентів.

В умовах ринкової конкуренції використовуються всілякі способи досягнення переваг, у тому числі збір інформації про інші організації. Все частіше трапляються випадки застосування нелегальних методів, що посилює жорсткість конкурентної боротьби. Адже без володіння інформацією про дії конкурента, передбачуваний попит на його продукцію, перспективні наукові розробки важко, а часом і неможливо бути конкурентоспроможним.

Згідно зі словником економічних термінів, комерційна таємниця – навмисно приховувані з комерційних міркувань економічні інтереси й відомості про різні сторони й сфери виробничо-господарської, управлінської, науково-технічної, фінансової діяльності фірми, охорона яких обумовлена інтересами конкуренції й можливими загрозами економічній безпеці фірми. Комерційна таємниця виникає тоді, коли вона становить інтерес для комерції.

При спробі захистити інформацію, що підпадає під комерційну таємницю, підприємство змушене вирішувати подвійне завдання: з одного боку, воно повинне рекламувати свою продукцію (послуги), а отже й інформувати постачальників і споживачів про свою діяльність, а з іншого – рекламувати без конкретної інформації, яка б розкрила багато аспектів діяльності підприємства, не можна, – і тут підприємство зіштовхується з проблемою розкриття комерційної таємниці.

Систематизовано і графічно представлені дані, що належать до комерційної таємниці підприємства.

Під підприємницьким шпигунством розуміють систему методів, прийомів і засобів збирання відомостей про виробництво, його діяльність і підприємців.

Підприємницьке шпигунство має на меті досягнення переваги в конкуренції будь-якими засобами, зміцнення своїх економічних позицій, одержання вигоди і заподіяння шкоди тому, чию комерційну таємницю використано

Однак інформація, як і інші економічні ресурси, є завжди обмеженою та суперечливою, тому управлінська діяльність на будь-якому підприємстві ведеться в умовах неповної та неточної інформації, тобто в умовах невизначеності. А це, у свою чергу, може призвести до виникнення загрози відхилення фактичних результатів від запланованих, ризику втрати конкурентних позицій на ринку та переходу лояльних споживачів до конкурентів. Тому менеджерам необхідно враховувати вплив невизначеності та породженого нею ризику на діяльність підприємства.

Невизначеність визначають як відсутність надійної інформації або недостатність відомостей про умови економічної діяльності та низький ступінь передбачуваності цих умов.

Проте слід мати на увазі і те, що саме підприємство ненавмисно спричиняє невизначеність ринку, приховуючи власну комерційну таємницю від суб'єктів недобросовісної конкуренції.

У роботі графічно представлена двозначна природа комерційної таємниці підприємства.

Розглянуто суперечливе значення комерційної таємниці.

Схематично представлені найпоширеніші способи втрати комерційної таємниці.

У другому розділі роботи проаналізовано організацію захисту комерційної таємниці на ТОВ «Стем».

Наведена загальна характеристика діяльності підприємства.

Товариство з обмеженою відповідальністю «Стем» (ТОВ «Стем») займається виробництвом металопластикових конструкцій.

Наведена організаційна структура управління підприємства.

Проаналізовано показники, що характеризують фінансові результати діяльності ТОВ «Стем» за 2019-2020 рр.

Чистий дохід від реалізації продукції збільшився у 2020 р. на 11,3 % і склав 154127,8 тис. грн. Собівартість продукції склала у 2020 р. 131298,3 тис. грн., що на 9,9 % вище рівня попереднього періоду.

Проаналізовано витрати підприємства за економічними елементами.

Сума операційних витрат на підприємстві зросла у 2020 р. на 20,8 % і склала 117898,9 тис. грн.

Наведена структура витрат на підприємстві у динаміці.

Графічно наведено динаміку витрат на ТОВ «Стем».

Чистий прибуток збільшився у 2020 р. на 2567,8 тис. грн., що склало 40,5 %.

Середньооблікова чисельність працівників збільшилася у 2020 р. на 9,6 % і склала 263 особи. Продуктивність праці у 2020 р. на підприємстві збільшилася на 17,8 % і склала 679,8 тис. грн./ос. Це свідчить про підвищення ефективності використання трудових ресурсів на підприємстві.

Рентабельність продажів збільшилася на 1,2 %. Це свідчить про підвищення ефективності діяльності підприємства в аналізованому періоді.

Графічно представлено динаміку основних показників, що характеризують фінансові результати діяльності ТОВ «Стем».

У результаті проведених досліджень можна зробити висновок про позитивну динаміку основних показників діяльності ТОВ «Стем» у 2019-2020 рр.

Також у даному розділі наведено характеристику напрямів забезпечення захисту комерційної таємниці на підприємстві.

Проаналізовано та представлено графічно загальні функції, що покладаються на службу безпеки підприємства.

Розглянуто особливості організації захисту комерційної таємниці в системі економічної безпеки ТОВ «Стем».

Наведений можливий перелік відомостей, що становлять комерційну таємницю підприємства і обслуговуючих організацій.

До загальних заходів захисту інформації в засобах і мережах їх передачі і обробки переважно передбачають використання апаратних, програмних та криптографічних засобів захисту. У свою чергу, апаратні засоби захисту застосовуються для вирішення таких завдань:

– перешкоджання візуальному спостереженню і дистанційному підслуховуванню;

– нейтралізація паразитних електромагнітних випромінювань і наводок;

– виявлення технічних засобів підслуховування і магнітного запису, несанкціоновано встановлених або які пронесено до установ підприємства, банку;

– захист інформації, що передається засобами зв'язку і знаходяться в системах автоматизованої обробки даних.

Складність визначення, яка саме інформація підприємства підлягає захисту, полягає в тому, що одна й та сама інформація в одному випадку вважатиметься конфіденційною, а в іншому – ні. Кожен підприємець самостійно визначає склад відомостей, що належатимуть до комерційної таємниці.

У третьому розділі роботи запропоновано шляхи підвищення організаційного забезпечення захисту комерційної таємниці на ТОВ «Стем».

Розроблено заходи щодо підвищення якості забезпечення захисту комерційної таємниці на підприємстві. В межах цього для досліджуваного підприємства запропоновано створити контррозвідувальний підрозділ у службі безпеки підприємства.

Це спеціальний підрозділ має організаційно бути складовою частиною служби безпеки, але в певному сенсі бути автономним. Він повинен мати свого керівника, який, підкоряючись голові служби безпеки, повинен мати самостійність через специфіку своїх обов'язків. Це припускає пряме й безпосереднє підпорядкування керівника контррозвідки голові служби безпеки.

Підрозділ контррозвідки повинен особливо піклуватися про спеціальну підготовку своїх співробітників. Діяльність контррозвідувального підрозділу фірми повинна узгоджуватися з вищим керівництвом і службовцями організації.

Важливим аспектом схоронності даних є ведення досьє. При цьому повинні використатися великі можливості електронної обробки й зберігання даних. У цих випадках завжди потрібно пам'ятати про уразливість запам'ятовувальних пристроїв ЕОМ і про необхідність дублювання даних шляхом запису їх на твердий носій або магнітну стрічку.

Для того, щоб одночасно забезпечити ефективність і безпеку інформації в умовах дії агентів шпигунства, життєво важливий гарний контроль за інформацією. Повинен бути організований твердий контроль за схоронністю документів у секретному відділі, особливо за досьє й розвідувальною інформацією.

Для досліджуваного підприємства необхідно приділити серйозну увагу заходам, пов'язаним з кадрами й запобіганням промисловому шпигунству, які наведені у вигляді схеми.

Також у даному розділі роботи запропоновано методику розробки проекту захисту комерційної таємниці на основі системного методу «OPSEC».

Для ефективного захисту комерційної таємниці на підприємстві керівники і працівники служби безпеки підприємства повинні розробити і реалізувати проект захисту комерційної таємниці.

Проект захисту комерційної таємниці на підприємстві – це унікальний комплекс взаємозв'язаних заходів, спрямованих на своєчасне виявлення і нейтралізацію причин і умов, сприяючих витоку комерційної таємниці в умовах обмежень за якістю, ресурсами, цілями, строками.

Системний підхід для вирішення поставлених питань доцільно представити у вигляді чітко формалізованої методики «OPSEC» (Operation Security). Даний метод має циклічний характер, оскільки після кожного етапу необхідно здійснювати його «самоконтроль» на предмет аналізу оптимальності прийнятих і проведених заходів.

Основні етапи процесу організації захисту інформації за методом «OPSEC» наведені графічно.

Запропоновано складання матриці відповідальності проекту захисту комерційної таємниці на підприємстві.

Впродовж розробки будь-якого проекту, завдяки певним особливостям проектної діяльності, на шляху його життєвого циклу будуть зустрічатися проектні ризики.

Проектні ризики – це сукупність ризиків, загрозливих реалізації інвестиційного проекту або здатних понизити його ефективність (комерційну, економічну, бюджетну, соціальну, економічну та ін.).

У табличній формі запропонована класифікація ризиків в процесі розробки проекту захисту комерційної таємниці на підприємстві з урахуванням фази проекту.

Для ефективної реалізації проекту велике значення має команда проекту. Необхідно розглядати процес утворення команди як створення єдиного, цілісного колективу управлінців, здатного ефективно досягати мети проекту. Командна кооперація персоналу дозволяє збільшити продуктивність управлінської праці на 70-80%.

Сферою використання запропонованих у роботі розробок є організація та управління системою фінансово-економічної безпеки підприємства.

Функціональне призначення – організаційно-правове забезпечення захисту комерційної таємниці на підприємстві.

Користувачами запропонованих рекомендацій можуть бути директор підприємства, заступники директора, начальник служби безпеки підприємства.

Можливими об’єктами практичного використання результатів дослідження можуть бути комерційні та некомерційні підприємства будь-якої форми власності та різних видів діяльності, посередницькі організації, фінансово-кредитні установи, страхові організації.

Основні результати досліджень опубліковані в роботах [76, 77].

Копії опублікованих праць наведено в додатку А.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мокрицька А. Б., Сліпченко Т. О. Економіко-правові аспекти захисту комерційної таємниці в Україні. *Бізнес Інформ*. 2018. № 12. С. 21-25.

2. Мулик Я. І., Григораш М. В. Роль внутрішньогосподарського контролю у збереженні комерційної таємниці. *Агросвіт*. 2018. № 8. С. 17-21.

3. Тугарова О. К., Шепета О. В. Організаційно-правові питання захисту комерційної таємниці. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2018. Вип. 52(2). С. 85-88.

4. Рева А. О. Щодо удосконалення механізму забезпечення нерозголошення комерційної таємниці працівником. *Журнал східноєвропейського права*. 2019. № 59. С. 181-187.

5. Турук А. О. Історичний аспект формування інституту комерційної таємниці. *Молодий вчений*. 2018. № 4(1). С. 92-95.

6. Кравченко О. М. Право Служби безпеки України та Національного антикорупційного бюро України на доступ до комерційної таємниці суб'єктів господарювання. *Інформаційна безпека людини, суспільства, держави*. 2018. № 1. С. 130-136.

7. Москаленко Н. О., Леонова Ю. О. Теоретичні підходи до конкурентної розвідки та особливості її аналітичного забезпечення. Проблеми економіки. 2018. № 2. С. 228-234.

8. Науменко М. О., Бережний Д. О. Управління фінансовим потенціалом підприємства на основі конкурентної розвідки. Вісник *економіки транспорту і промисловості*. 2019. № 67. С. 196-201.

9. Горбаль Н. І., Смерека Л. В., Микитин О. З. Конкурентна розвідка: сутність, значення, перспективи розвитку. *Management and entrepreneurship in Ukraine: the stages of formation and problems of development*. 2019. Vol. 1. numb. 2. С. 53-60.

10. Ланде Д. В. Правові питання конкурентної розвідки. *Інформація і право*. 2020. № 2. С. 51-68.

11. Мандзіновська Х. О. Управління фінансово-економічної безпекою: підручник / ред.Онищенко В. О. та ін. Полтава: ПолтНТУ, 2018. 530 с.

12. Козаченко Г. В., Рамазанов С. К., Ляшенко О. М., Погорелов Ю. С., Пшик Б. І. Система економічної безпеки: держава, регіон, підприємство: монографія [у 3 т.]. Т. 3. Луганськ: Промдрук, 2014. 336 с.

13. Франчук В. І. Економічна безпека суб'єктів господарської діяльності: підручник; Львів. держ. ун-т внутр. справ. Львів, 2015. 235 с.

14. Майстро Р.Г., Полозова Т.В. Напрями вдосконалення державного регулювання економічної безпеки України. *Приазовський економічний вісник*. 2019. Випуск 1(12). С. 46-50.

15. Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2020. № 4. С. 68-73.

16. Нашинець-Наумова А. Ю. Правова охорона комерційної таємниці в сфері підприємницької діяльності. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. 2019. Т. 30(69). № 2. С. 85-89.

17. Гомотюк О., Сліпченко Т. Генезис правового регулювання відносин у сфері захисту комерційної таємниці. *Актуальні проблеми правознавства*. 2018. Вип. 3. С. 82-86.

18. Зайцева-Калаур І. Організаційно-правові процедури забезпечення охорони та захисту комерційної таємниці суб’єкта господарювання. *Актуальні проблеми правознавства*. 2018. Вип. 4. С. 110-115.

19. Завертнева-Ярошенко В. А., Ячменська М. М. Проблеми правового захисту комерційної таємниці в Україні. *Правова держава*. 2018. № 32. С. 134-145.

20. Свинарчук В. М. Комерційна таємниця як вид інформації з обмеженим доступом: аналіз законодавчої практики. *Інформація і право*. 2019. № 3. С. 50-54.

21. Руденко Л. Д. Правова охорона інновацій у режимі комерційної таємниці, промислової власності: порівняльний аналіз. *Вісник Харківського національного університету внутрішніх справ*. 2020. № 2. С. 189-197.

22. Лук'янова В. В., Шутяк Ю. В. Діагностика економічної безпеки підприємства: монографія. Хмельницький: ХНУ, 2014. 165 с.

23. Карпенко Н. Г. Комерційна таємниця – визнання, захист, відповідальність. *Ефективна економіка*. 2020. № 5. Режим доступу: http://nbuv.gov.ua/UJRN/efek_2020_5_41.

24. Полінкевич О. М. Стратегії управління економічною безпекою підприємств. *Економічний форум*. 2018. № 2. С. 251-257.

25. Меліхова Т. О. Економічна безпека промислових підприємств: аналіз фінансового стану, ймовірності банкрутства, чистого економічного ефекту від залучення інвестицій. *Вісник Приазовського державного технічного університету. Серія: Економічні науки*. 2018. Вип. 35. С. 213-221.

26. Редько К. Ю., Куніцька З. Е. Комерційна таємниця: особливості та проблеми нормативно-правового забезпечення в Україні. Державне управління: удосконалення та розвиток. 2021. № 5. Режим доступу: http://nbuv.gov.ua/UJRN/Duur_2021_5_11.

27. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур: Монографія. Львів: ЛБІ НБУ, 2004. 195 с.

28. Толпежніков Р. О., Толпежнікова Т.Г., Балашов М.І. Методологічні підходи до управління змінами в стратегії забезпечення потенціалу економічної безпеки промислових підприємств. *Менеджер*. 2019. № 4. С. 56-63.

29. Фінансово-економічна безпека: стратегічна аналітика та аудиторський супровід: монографія / ред.: Т. В. Момот; Харків. нац. ун-т

міськ. госп-ва ім. О. М. Бекетова. Харків: ХНУМГ ім. О. М. Бекетова, 2015. 340 с.

30. Костіна О. М., Майборода О. Є. Методи та моделі діагностики кризового стану підприємства. *Вісник СумДУ*. 2012. № 4. С. 91-97.

31. Момот Т. В., Шаповал Г. М., Панов В. В. Стратегічний моніторинг в системі забезпечення фінансово-економічної безпеки підприємства. *Вісник Хмельницького національного університету. Економічні науки.* 2017. № 3(1). С. 80-84.

32. Полозова Т.В., Журавель М. Ю. Процес забезпечення економічної безпеки підприємства. *Економіка: проблеми теорії та практики: Збірник наукових праць*. Випуск 255: В 9 т. Т. VI. Дніпропетровськ: ДНУ, 2009. С. 1454-1459.

33. Живко З. Б. Управління системою економічної безпеки підприємства: навч. посіб.; Львів. держ. ун-т внутр. справ. Львів, 2016. 211 с.

34. Полозова Т. В., Журавель М. Ю. Організаційне забезпечення складових економічної безпеки підприємства. *Економіка: проблеми теорії та практики: Збірник наукових праць*. Випуск 257: В 7 т. Т. III. Дніпропетровськ: ДНУ, 2009. С. 613-619.

35. Копча Ю. Ю. Науковий підхід до формування стратегічних орієнтирів управління потенціалом економічної безпеки підприємств. *Бізнес Інформ*. 2019. № 7. С. 330-336.

36. Герасименко Т. О., Мазуренко О. М. Аналіз господарської діяльності: навч. посіб.; Львів. комерц. акад. Львів, 2014. 319 с.

37. Божидарнік Т. В., Кривов'язюк І. В. Обґрунтування господарських рішень і діагностика промислового підприємства: сучасний формат: монографія; Луц. нац. техн. ун-т. Луцьк, 2014. 160 с.

38. Міщук Г. Ю., Джигар Т. М., Шишкіна О. О. Економічний аналіз: навч. посіб.; Нац. ун-т вод. госп-ва та природокористування. Рівне: НУВГП, 2017. 155 с.

39. Могилевська О. Ю., Уфімцева Т. М., Слободяник А. М. Економіка підприємства. Теорія і практика : навч. посіб.; Київ. міжнар. ун-т. Київ, 2017. 295 с.

40. Ковальчук І. В. Економіка підприємства: навч. посібник. Київ: Знання, 2014. 679 с.

41. Основи економічного аналізу: навч.-метод. посіб. для студентів екон. спец., магістрів, аспірантів, викл. / В. М. Микитюк та ін.; ред. В. М. Микитюк; Житомир. нац. агроекол. ун-т. Житомир: Рута, 2018. 439 с.

42. Шарко М. В., Мєшкова-Кравченко Н. В., Радкевич О. М. Економіка підприємства: навч. посіб. для студ. ВНЗ. Ч. 1; Херсон. нац. техн. ун-т. Херсон, 2014. 434 с.

43. Череп А. В., Ярмош В. В. Економіка підприємства: підручник; ДВНЗ «Запоріз. нац. ун-т». Запоріжжя: ЗНУ, 2014. 335 с.

44. Семенда Д. К., Бурляй О. Л., Коротєєв М. А., Семенда О. В. Економіка підприємства: підруч. для студентів ВНЗ; ред.: Д. К. Семенда; Уман. нац. ун-т садівництва. Умань: Сочінський, 2014. 477 с.

45. Череп А. В., Худолєй Л. В. Використання інструментів забезпечення фінансово-економічної безпеки промислових підприємств: монографія; Запоріз. нац. ун-т. Запоріжжя: Запоріз. нац. ун-т, 2018. 221 с.

46. Єфдокимов В. В., Олійник О. В., Грицишен Д. О., Грищенко О. О. Концепція управління економічною безпекою суб'єктів господарювання в контексті теорії сталого розвитку: монографія; Житомир. держ. технол. ун-т. Житомир, 2013. 251 с.

47. Комплексне забезпечення фінансово-економічної безпеки: навч. посіб. для студентів ВНЗ / ред. Г. Є. Павлова та ін. Дніпро: Акцент, 2018. 559 с.

48. Компанієць Д. О. Конкурентна розвідка як маркетинговий інструмент сучасного бізнесу. *Часопис Національного університету*

«Острозька академія». Сер.: Право. 2013. № 2. Режим доступу: http://nbuv.gov.ua/UJRN/Choasp_2013_2_20.

49. Мазаракі А. А., Корольчук О. П., Мельник Т. М. Економічна безпека України в умовах глобалізаційних викликів: монографія; Ред.: А. А. Мазаракі; Київ. нац. торг.-екон. ун-т. К., 2010. 717 с.

50. Лопатка К. А., Рогожина Д. Д. Бізнес-планування як ефективний інструмент реалізації стратегії підвищення економічної безпеки підприємства. *Економічний простір*. 2020. № 158. С. 46-49.

51. Петряєва З. Ф. Забезпечення фінансово-економічної безпеки стратегічного розвитку підприємства. *Молодий вчений*. 2019. № 10(1). С. 319-325.

52. Коптєва Г. М. Стратегічне планування як процес забезпечення економічної безпеки бізнес-процесів підприємства торгівлі. *Бізнес-навігатор*. 2020. Вип. 3. С. 95-100.

53. Штангрет А. М., Караїм М. М., Штангрет І. А. Інтенсифікація управління економічною поведінкою підприємства: безпекові засади. *Ефективна економіка*. 2020. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2020_5_8.

54. Polozova T.V., Nicola Jennifer John Elia. Enterprise economic security system: theoretical aspects of formation. Економічні та безпекові виклики сучасного бізнес-середовища: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2020. С. 355-362.

55. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету. Економічні науки.* 2020. № 4(1). С. 32-35.

56. Квасній Л. Г., Попівняк О. М., Щербан О. Я. Стратегічне і тактичне планування діяльності підприємства як основні складові механізму забезпечення його економічної безпеки. *Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського. Економічні науки*. 2015. № 1. С. 48-53.

57. Христофоров В. О., Андрющенко Є. Г. Формування механізмів забезпечення економічної безпеки підприємств. *Вісник ХНАУ. Серія: Економічні науки.* 2019. № 1. С. 328-336.

58. Беззубченко О. А. Економічна безпека як складова стратегії розвитку підприємства в умовах нестабільності. *Вісник Маріупольського державного університету. Серія: Економіка*. 2020. Вип. 19. С. 20-27.

59. Вдовиченко Л. Ю., Волосюк М. В. Теоретико-методологічні аспекти формування механізму стратегічного управління економічною безпекою підприємства. *Бізнес Інформ*. 2020. № 10. С. 469-477.

60. Polozova T., Musiienko V., Storozhenko O., Peresada O., Geseleva N. Modeling of energy-saving processes in the context of energy safety and security. *Journal of security and sustainability issues*. 2019. № 8 (3). С. 387-397.

61. Новик І. В. Проблеми та перспективи забезпечення економічної безпеки підприємства в Україні. *Інфраструктура ринку*. 2020. Вип. 43. С. 229-233.

62. Ольшанський О. В., Крамчанінова М. Д. Вплив пандемії COVID-19 на проблеми забезпечення економічної безпеки малих та середніх підприємств. *Економічний вісник Донбасу*. 2021. № 2. С. 78-82.

63. Управління фінансовою безпекою економічних суб'єктів: навч. посіб. для студентів ВНЗ екон. і юрид. спец. усіх форм навчання / ДВНЗ «Укр. акад. банк. справи Нац. банку України», Каф. фінансів; за заг. ред. д-ра екон. наук, проф. С. М. Фролова; [уклад.: С. М. Фролов та ін.]. Суми: ДВНЗ «УАБС НБУ», 2015. 331 с.

64. Лясковець О. В. Теоретико-методичні основи забезпечення стратегічного управління розвитком економічної безпеки підприємств машинобудування. *Вісник Хмельницького національного університету. Економічні науки*. 2018. № 2. С. 129-134.

65. Онищенко С. В., Пугач О. А. Загрози економічній безпеці України: сутність, оцінювання та механізм упередження: монографія. Полтава: ПолтНТУ, 2015. 337 с.

66. Злотенко О. Б. Стратегічні орієнтири забезпечення економічної безпеки інвестиційної діяльності промислових підприємств. *Вісник Київського національного університету технологій та дизайну. Серія*: Економічні науки. 2019. № 2. С. 100-107.

67. Клевчік Л. Л. Стратегічне управління фінансовою безпекою підприємства. *Науковий вісник Чернівецького університету. Економіка*. 2017. Вип. 794. С. 51-57.

68. Концептуальні засади формування фінансово-економічної безпеки: колект. монографія / [Абакуменко О. І. та ін.]; за заг. ред. д-ра екон. наук, проф. Шкарлета Сергія Миколайовича; Черніг. нац. технол. ун-т. Ніжин: Лук'яненко В.В.: Орхідея, 2015. 440 с.

69. Іващенко В. Основи методики розслідування незаконного збирання та розголошення комерційної таємниці. *Юрид. журн*. 2006. № 8. С. 32-35.

70. Єпіфанов А. О., Пластун О. Л., Домбровський В.С., Болгар Т. М., Ващенко О. М. Фінансова безпека підприємств і банківських установ: монографія; Ред.: А. О Єпіфанов. Суми: ДВНЗ «УАБС НБУ», 2009. 295 с.

71. Меліхова Т. О. Вдосконалення функцій та завдань забезпечення економічної безпеки підприємств. *Інвестиції: практика та досвід*. 2018. № 3. С. 70-73.

72. Топоркова О. В., Акімова Н. С., Наумова Т. А. Стратегічні аспекти управління ризиками для забезпечення економічної безпеки підприємства. *Бізнес Інформ*. 2019. № 8. С. 237-243.

73. Стратегія та механізми забезпечення фінансово-економічної безпеки: колект. монографія / Чернігів. нац. технол. ун-т ; за заг. ред. д-ра екон. наук, проф. Ільчука Валерія Петровича. Чернігів: ЧНТУ, 2017. 349 с.

74. Ілляшенко С.М. Економічний ризик: навч. посіб. 2-ге вид., доп., перероб. Київ: Центр навчальної літератури, 2004. 220 с.

75. Клебанова Т. С. Математичні методи і моделі ринкової економіки: навч. посіб. / Т.С. Клебанова, М.О. Кизим, О.І. Черняк, О.В. Раєвнєва, К.А. Стрижиченко, Л.С. Гур'янова, О.В. Мілов, О.А. Сергієнко, О.Ю. Полякова, Н.А. Дубровіна; Харк. нац. екон. ун-т. Харків: Інжек, 2014. 456 с.

76. Полозова Т. В., Сеїдова Г. М. Теоретичні аспекти захисту комерційної таємниці на підприємстві. *Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта.* Матеріали II Міжнародної науково-практичної конференції (м. Харків, 2 листопада 2021 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2021. С. 135-136.

77. Полозова Т. В., Сабіров С. С., Сеїдова Г. М. Формування стратегії забезпечення економічної безпеки підприємства. Сучасні економічні стратегії: інновації, безпека та сталий розвиток: колективна монографія / За заг. ред. д.е.н., проф. Т.В. Полозової, д.е.н., проф. І.В. Колупаєвої, к.е.н., доц. О.В. Мурзабулатової Харків: ХНУРЕ, 2021. С. 272-281.