МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, доцент	доктор економічних наук, доцент
_____ С.В.Легомінова	_____ С.В.Легомінова
«___»_____20__ р.	«___»_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему:

КОНКУРЕНТНА РОЗВІДКА ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ: Калініченко Ігор Андрійович _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.е.н., доц. Мордас Ірина Василівна _____
(підпис)

Київ – 2020

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
«_____»_____ 2020 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Калініченку Ігору Андрійовичу

1 **Тема роботи**: «КОНКУРЕНТНА РОЗВІДКА ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА», затверджена наказом по університету № ___ від «___»_____ 2019 р.

2 **Термін здачі** студентом оформленої роботи «___» _____ 2019 р.

3 **Об'єкт дослідження:** забезпечення інформаційної безпеки підприємства.

4 **Предмет дослідження:** конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства.

5. **Мета дослідження** полягає у вивченні засад конкурентної розвідки як складової забезпечення інформаційної безпеки підприємства.

5 **Перелік питань, які мають бути розроблені:**

5.1 Встановити особливості забезпечення інформаційної безпеки підприємства в умовах конкурентної боротьби в інформаційній сфері.

5.2 Дослідити основні засади конкурентної розвідки: цілі, етапи і методи.

5.3 Розглянути практичні аспекти впровадження конкурентної розвідки на підприємстві.

5.4 Проаналізувати програмні засоби конкурентної розвідки і розробити рекомендації щодо застосування методів конкурентної розвідки у контексті забезпечення інформаційної безпеки підприємства.

6 **Дата видачі завдання «**16» вересня 2019 р.

Науковий керівник Т.М. Мужанова

_____
підпис

Завдання прийнято до виконання І.А. Калініченко

_____
підпис

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Калініченком Ігорем Андрійовичем

Дата видачі завдання: «16» вересня 2019 р.

№ з/п	Етапи магістерської атестаційної роботи	Термін виконання етапів	Примітка
	Визначення об'єкта, предмета, мети та завдань дослідження.	16.09.2019	
	Збір та аналіз літератури.	27.09.2019	
	Вивчення особливостей забезпечення інформаційної безпеки підприємства в умовах конкурентної боротьби	11.10.2019	
	Дослідження основних засад конкурентної розвідки	25.10.2019	
	Вивчення практичних аспектів впровадження конкурентної розвідки на підприємстві	08.11.2019	
	Аналіз і розробка рекомендацій щодо застосування методів конкурентної розвідки у контексті забезпечення інформаційної безпеки	22.11.2019	
	Формулювання висновків за результатами проведеного дослідження.	06.12.2019	
	Оформлення роботи.	13.12.2019	
	Оформлення презентації.	20.12.2019	
.	Отримання рецензії на роботу.	26.12.2019	
.	Захист у ДЕК.	14.01.2020	

Студент І.А.Калініченко
(підпис)

Науковий керівник Т.М.Мужанова
(підпис)

РЕФЕРАТ

Магістерська атестаційна робота присвячена дослідженню засад конкурентної розвідки як складової забезпечення інформаційної безпеки підприємства. Робота складається зі вступу, чотирьох розділів, що містять 12 рисунків і таблицю, висновки та списку використаних джерел з 47 найменувань. Загальний обсяг роботи становить 87 аркушів, з яких 4 аркуша займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства.

Метою роботи є вивчення засад конкурентної розвідки як складової забезпечення інформаційної безпеки підприємства.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, теорій менеджменту персоналу й інформаційної безпеки.

Як результат у роботі встановлено особливості забезпечення інформаційної безпеки підприємства в умовах конкурентної боротьби в інформаційній сфері досліджено основні засади конкурентної розвідки, зокрема цілі, етапи та методи; розглянуто практичні аспекти впровадження конкурентної розвідки на підприємстві; проаналізовано програмні засоби конкурентної розвідки і розроблено рекомендації щодо застосування методів конкурентної розвідки у контексті забезпечення інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при організації та впровадженні комплексу заходів конкурентної розвідки підприємства у контексті забезпечення корпоративної інформаційної безпеки.

Ключові слова: ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ, КОНКУРЕНТНА РОЗВІДКА, МЕТОДИ КОНКУРЕНТНОЇ РОЗВІДКИ, ЗАСОБИ КОНКУРЕНТНОЇ РОЗВІДКИ.

ЗМІСТ

ВСТУП

Актуальність теми. Ефективність функціонування сучасного підприємства в умовах ринкової конкуренції значною мірою залежить не тільки від захисту конфіденційної інформації та засобів її обробки, але й від наявності в розпорядженні керівництва та використання різноманітної бізнес-інформації для прийняття своєчасних та обгрунтованих управлінських рішень, а в кінцевому рахунку - для формування конкурентної стратегії розвитку підприємства. Водночас, конкурентна розвідка є важливим елементом забезпечення інформаційної безпеки підприємства, створюючи передумови для захисту його інформаційних інтересів через професійну і послідовну інформаційно-аналітичну діяльність, яка є основою ефективного управління.

Отже, дослідження засад конкурентної розвідки як засобу забезпечення конкурентноспроможності бізнесу загалом та інформаційної безпеки підприємства зокрема є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад конкурентної розвідки як складової забезпечення інформаційної безпеки підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Встановити особливості забезпечення інформаційної безпеки підприємства в умовах конкурентної боротьби в інформаційній сфері.
2. Дослідити основні засади конкурентної розвідки: цілі, етапи і методи.
3. Розглянути практичні аспекти впровадження конкурентної розвідки на підприємстві.
4. Проаналізувати програмні засоби конкурентної розвідки і розробити рекомендації щодо застосування методів конкурентної розвідки у контексті забезпечення інформаційної безпеки підприємства.

Об’єкт дослідження - забезпечення інформаційної безпеки підприємства.

Предмет дослідження – конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи теорії менеджменту та конкуренції, методи аналізу, синтезу та порівняння, концепції розвідувальної діяльності.

Наукова новизна одержаних результатів. Розроблені підходи

можуть бути використані при плануванні та реалізації заходів конкурентної розвідки підприємства у контексті забезпечення інформаційної безпеки.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу підприємству виробити адекватний підхід до впровадження конкурентної розвідки на підприємстві, а також здійснити обґрунтований вибір методів і засобів збору й аналізу інформації в рамках впровадження заходів із забезпечення інформаційної безпеки.

Розділ 1
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ КОНКУРЕНТНОЇ БОРОТЬБИ

1.1 Основні підходи до забезпечення інформаційної безпеки підприємства

У процесі своєї діяльності будь-яке підприємство оперує інформацією як специфічним товаром високої цінності. Володіння інформацією, її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу.

З огляду на зростаючі обсяги інформації, переведення значної її частини в електронну форму, використання інформаційних систем, локальних і глобальних мереж у всіх сферах діяльності людини, виникають якісно нові загрози інформації, а вирішення завдань щодо її зберігання, передачі та обробки є надзвичайно актуальним.

Сучасний діловий світ, представлений головним чином фінансово-інформаційними корпораціями, страждає від інформаційної крадіжки. За даними світової статистики, втрата тільки 20% інформації веде до руйнування 65% фірм і компаній. Тому забезпечення інформаційної безпеки (далі - ЗІБ) є одним із найважливіших показників успішної діяльності організації [1].

Очевидно, що сьогодні для досягнення стану захищеності підприємства від внутрішніх та зовнішніх інформаційних загроз необхідним є здійснення активної, цілеспрямованої і послідовної діяльності, впровадження сукупності заходів і використання комплексу різноманітних засобів ЗІБ.

Виходячи із тлумачення слова «забезпечувати» (створювати надійні умови для здійснення чого-небудь; гарантувати щось), метою діяльності із забезпечення ІБ підприємства є створення умов для збереження цілісності, повноти та точності інформації, мінімізація ризику несанкціонованих змін у корпоративних інформаційних системах [2].

Також ЗІБ підприємства визначають як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [3].

ЗІБ підприємства характеризується конфіденційністю, цілісністю, доступністю та може розглядатися як сукупність таких елементів: безпечні умови функціонування ІТ, побудова ефективної інфраструктури інформаційного простору, цілісного ринку інформації, створення оптимальних умов для проходження інформаційних процесів.

До основних цілей ЗІБ належать:

• запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;

• запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації;

• запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об’єкту власності;

• захист прав суб’єктів підприємницької діяльності, а також громадян на збереження їх конфіденційної інформації, наявної в інформаційних системах;

• збереження конфіденційності документованої інформації відповідно до законодавства [4].

На думку фахівців, ЗІБ підприємства передбачає наявність трьох складових: діяльність, засоби та суб’єкти (Рис.1.1).

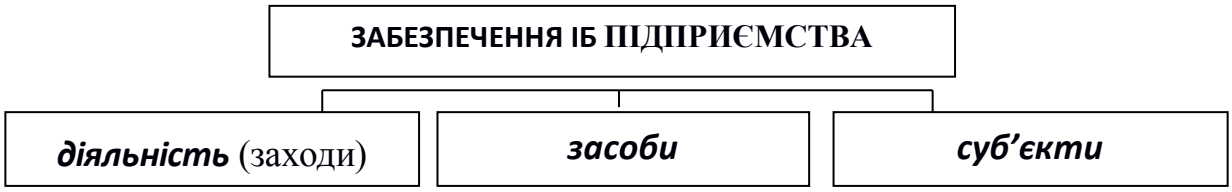

Рис. 1.1. Структура забезпечення ІБ підприємства.

Діяльність із ЗІБ. Діяльність щодо ЗІБ є сукупністю різноманітних заходів, які спрямовані на задоволення основних потреб та досягнення цілей підприємства у сфері ІБ із використанням відповідних матеріальних, духовних, фінансових, правових, організаційних, технічних та інших засобів.

Загалом заходи, орієнтовані на ЗІБ підприємства, можуть бути охарактеризовані цілим рядом параметрів, що відображають напрями

діяльності, орієнтацію на об'єкти ЗІБ, характер загроз, способи дій, їх поширеність, охоплення і масштабність (Рис 1.2.).

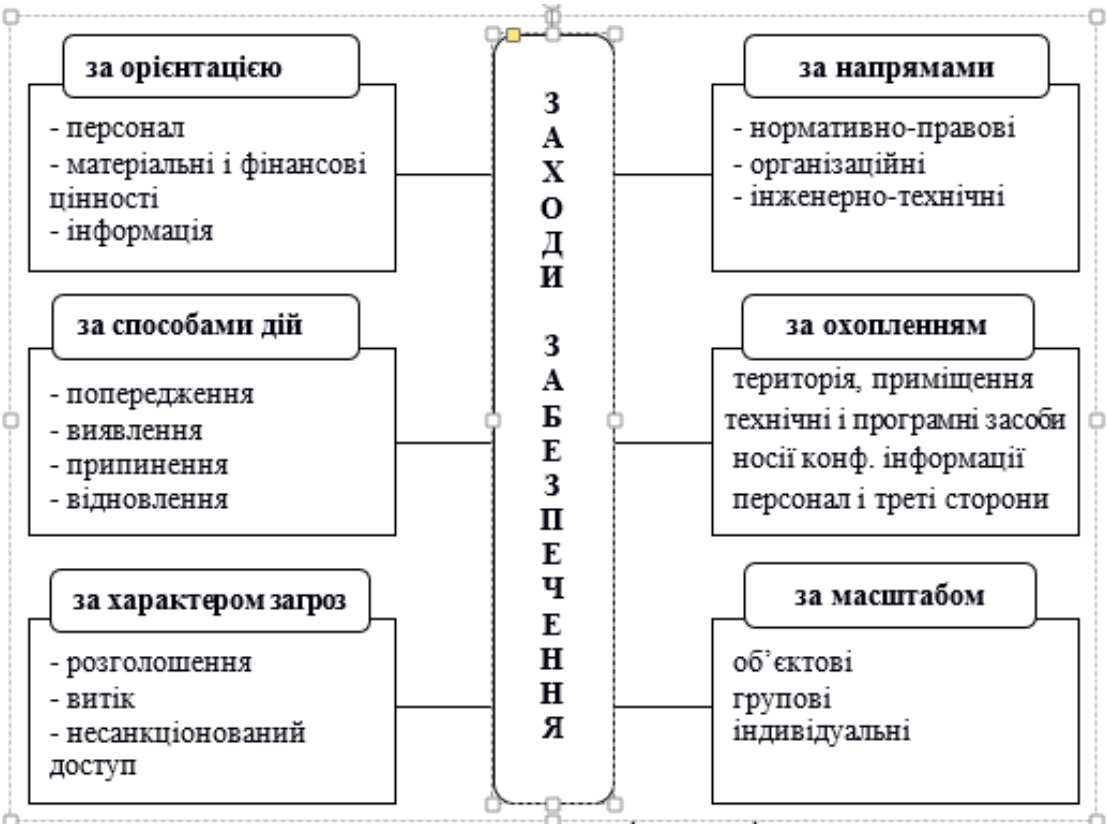

Рис. 1.2. Види заходів ЗІБ підприємства.

Так, за характером загроз заходи ЗІБ орієнтовані на запобігання розголошенню, витоку і несанкціонованому доступу до конфіденційної інформації підприємства та її носіїв.

За орієнтацією на об'єкти виділяють заходи щодо ЗІБ персоналу підприємства, його матеріальних і фінансових цінностей, інформації та її матеріальних носіїв.

За способами дій заходи можна поділити на заходи із метою запобігання, виявлення, припинення (загроз) і відновлення (ресурсів, ІТКС тощо).

Заходи ЗІБ можна охарактеризувати за масштабністю як об'єктові (здійснюються в масштабах усього підприємства, окремих його об'єктів), групові або індивідуальні [5].

За охопленням заходи із ЗІБ можуть бути орієнтовані на територію, будівлю, приміщення, технічні та програмні засоби або їх окремі елементи, носії конфіденційної інформації, які належать підприємству, а також персонал і всіх суб'єктів, задіяних у системі ЗІБ підприємства.

За напрямами здійснення всі заходи із ЗІБ підприємства поділяють на: нормативно-правові; організаційні; програмні-технічні. Деякі фахівці додають до зазначених видів морально-етичні та фізичні заходи [5].

До нормативно-правових заходів ЗІБ підприємства належать застосування законів, указів, положень, інструкцій та інших нормативних актів загальнодержавної чи галузевої дії, а також розробка і впровадження внутрішніх нормативних документів підприємства, які регламентують правила поводження з інформацією обмеженого використання і відповідальності за їх порушення.

Морально-етичні заходи передбачають формування та заохочення персоналу підприємства до дотримання різноманітних норм поведінки (які традиційно склалися або складаються в суспільстві загалом і в межах підприємства зокрема), які запобігають виникненню загроз ІБ підприємства та сприяють безпечному поводженню персоналу у випадках їх реалізації. Ці норми бувають як неписаними (загальновизнані норми чесності, корпоративної відданості тощо), так і оформленими у вигляді зводу правил чи приписів.

До заходів фізичного ЗІБ відносять встановлення й використання різних механічних, електричних і електромеханічних пристроїв або споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу порушників (турнікети, колючий дріт, кодові замки, системи охоронно-пожежної сигналізації тощо).

Заходи програмно-технічного ЗІБ підприємства включають встановлення та функціонування різних електронних пристроїв та спеціальних програм, які самостійно або в комплексі з іншими заходами унеможливлюють витік, знищення та блокування інформації, порушення цілісності та режиму доступу до неї [6]: ідентифікацію і аутентифікацію суб'єктів інформаційної системи; розмежування доступу до ресурсів; контроль цілісності даних; забезпечення конфіденційності даних; аудит подій, що відбуваються в інформаційній системі; резервування її ресурсів та компонентів.

Говорячи про організаційні заходи із ЗІБ підприємства, слід згадати про організацію як функцію управління діяльністю підприємства, котра є видом управлінської діяльності і спрямовується на розподіл завдань між виконавцями.

Загалом організаційна діяльність - це сукупність процесів, за допомогою яких керівництво організації може вирішити проблеми чи усунути конфлікти. Основними складовими організаційної діяльності є: розподіл праці, розподіл ресурсів, делегування повноважень, встановлення контролю за виконанням робіт, створення механізмів координації [7].

Відповідно організаційні (організаційно-адміністративні) заходи ЗІБ підприємства регламентують (через відзначені вище складові) процеси функціонування інформаційних систем; використання інформаційних ресурсів; діяльність персоналу служби ІБ і працівників підприємства загалом; порядок взаємодії користувачів із системою тощо.

Засоби ЗІБ. Аналізуючи засоби ЗІБ підприємства, варто зазначити, що для їх систематизації та класифікації доцільно використати висвітлені вище підходи, зокрема за сукупністю параметрів, що відображають напрями діяльності, орієнтацію на об'єкти забезпечення ІБ, характер загроз, способи дій, їх поширеність, охоплення і масштабність.

Однією із найбільш показових є класифікація засобів ЗІБ на нормативно-правові, організаційні та програмно-технічні [5] (Рис. 1.3.)

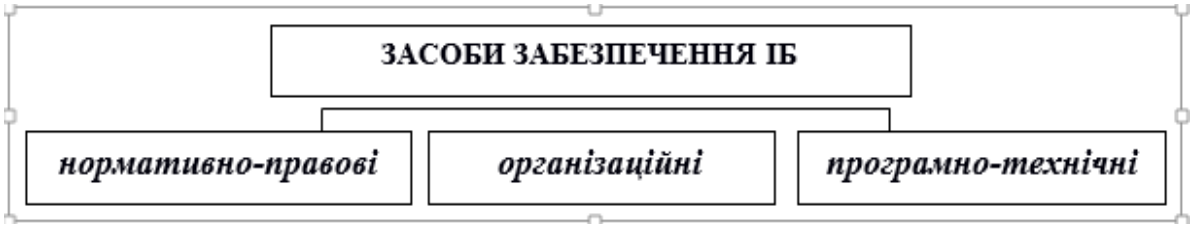

Рис. 1.3. Види засобів ЗІБ підприємства.

До нормативно-правових засобів ЗІБ підприємства належать законодавчі та нормативні документи у сфері ІБ та дотичних сферах (в тому числі стандарти та специфікації), діючі на рівні держави, галузі чи регіону, а також внутрішні нормативні документи підприємства (політики, інструкції, процедури тощо).

Засоби програмно-технічного ЗІБ підприємства включають різноманітні електронні пристрої та спеціальні програми.

До організаційних засобів відносять методи, способи і прийоми, за допомогою яких здійснюється організаційна діяльність у сфері нормативного, програмно-технічного, фізичного та інших аспектів ЗІБ, зокрема засоби планування, інструктування, координації, контролю, вироблення управлінських

рішень, надання допомоги, забезпечення своєчасного виконання завдань, сприяння проведенню відповідних заходів за зазначеними вище напрямами тощо [7].

Сутність організаційних засобів та методів полягає у впорядкуванні діяльності структурних підрозділів та персоналу підприємства з метою їх оптимального функціонування. Ці засоби спрямовані як всередину структури, на підвищення організованості та оптимізацію діяльності підприємства загалом і служби ІБ зокрема, так і на підвищення ефективності практичної реалізації ними своїх завдань та функцій.

Організаційні засоби використовують для регламентації процесів функціонування інформаційних систем; використання інформаційних ресурсів; діяльності персоналу служби ІБ і працівників підприємства загалом; взаємодії користувачів із системою тощо.

Крім відзначених трьох основних видів засобів ЗІБ підприємства виділяють ще морально-етичні засоби: загальносуспільні і корпоративні норми поведінки (формально зафіксовані і так звані «неписані»).

Суб'єкти ЗІБ. Характеризуючи систему суб'єктів ЗІБ підприємства, слід відзначити наявність кількох рівнів:

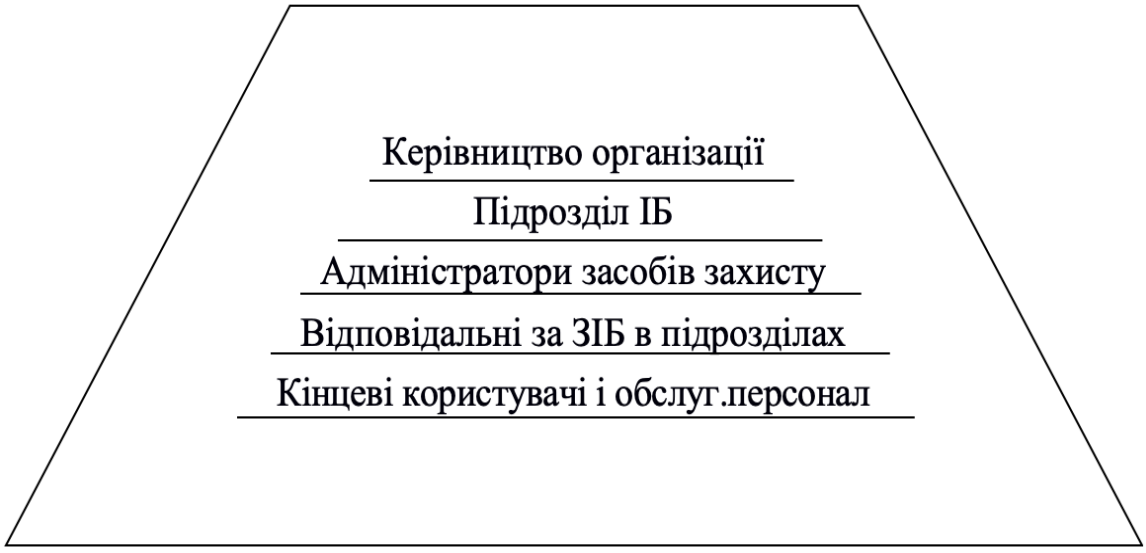

Рис. 1.4. Рівні суб'єктів ЗІБ підприємства.

Розглядаючи структуру служби, яка відповідає за ЗІБ підприємства, доцільно відзначити необхідність формування таких підрозділів у її складі:

– підрозділу режиму і охорони;

– спеціального підрозділу обробки документів конфіденційного характеру;

– інженерно-технічних підрозділів;

– інформаційно-аналітичних підрозділів.

Можливою є наявність підрозділу конкурентної розвідки та контррозвідки [8].

У складі служби ІБ для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій:

– відділ нормативної (організаційної) документації;

– відділ адміністрування інформаційних систем;

– відділ впровадження інформаційних систем і систем захисту інформації;

– відділ аудиту ІБ [9].

Фахівці з питань ІБ [6] акцентують на необхідності залучення фахівців таких спеціальностей до складу служби ІБ підприємства, як юрист; аналітик; спеціалісти у сфері управління ІБ, економічної розвідки, контррозвідки; технічні фахівці у сфері захисту інформації; співробітники охорони та пропускного режиму.

Важливим є дотримання принципу підпорядкування керівника служби ІБ безпосередньо керівнику підприємства; надання заступнику керівника служби функцій управління системами фізичного і технічного захисту підприємства.

Здійснюючи діяльність із забезпечення ІБ, важливо усвідомлювати, що крім власного персоналу, на ІБ підприємства можуть впливати треті особи й організації, як партнерські, так і ті, що мають за мету втручання в процес функціонування систему ІБ підприємства або несанкціонованого доступу до його інформації як локально, так і віддалено.

Таким чином, систему забезпечення ІБ підприємства можна визначити як сукупність організаційних, нормативних, технічних, програмних заходів, які впроваджуються з метою гарантувати конфіденційність, цілісність і доступність інформації, виходячи з вимог бізнесу.

Узагальнивши різні наукові підходи [9,6,10,11,12], можна виділити такі загальні принципи ЗІБ:

– принцип комплексного підходу, тобто ефективне використання сил, засобів, способів і методів ІБ для вирішення поставлених завдань залежно від конкретної ситуації;

– принцип адаптивності означає пристосовуваність системи забезпечення ІБ до швидко змінних оточуючих підприємство умов та загроз і передбачає здійснення постійного всебічного аналізу функціонування системи ІБ з метою прийняття своєчасних заходів щодо пристосування до динамічно змінної ситуації та підвищення її ефективності;

– принцип оперативності ухвалення управлінських рішень (істотно впливає на ефективність функціонування і гнучкість системи захисту інформації і відображає націленість керівництва і персоналу підприємства на вирішення задач захисту інформації);

– принцип ефективності, що означає дотримання оптимального балансу між можливостями, продуктивністю і витратами системи забезпечення ІБ;

– принцип економічної доцільності, відповідно до якого обсяги витрат на забезпечення ІБ не можуть перевищувати розміру збитків у випадку реалізації потенційних загроз.

Крім того забезпечення ІБ має бути складовою системи управління організацією, бути узгодженим із її бізнес-завданнями і стратегією, здійснюватися централізовано за умов однозначної підтримки і зобов’язань з боку керівництва організації, гарантувати повне дотримання керівництвом і персоналом встановлених норм та правил забезпечення ІБ, а також здійснення обліку й контролю за діяльністю у системі забезпечення ІБ із використанням зворотного зв’язку.

З метою протидії негативним проявам т.зв. «людського фактора» ЗІБ має здійснюватися на засадах:

– персональної відповідальності (найбільш ефективний розподіл завдань із забезпечення ІБ між керівництвом і персоналом підприємства і визначення відповідальності за повноту та якість їх виконання);

– розподілу обов'язків (такий розподіл ролей та відповідальності, щоб одна людина не могла порушити критично важливий для ІБ підприємства процес);

– мінімізації привілеїв (виділення користувачам тільки тих прав доступу, які необхідні їм для виконання службових обов'язків);

– постійного навчання й обізнаності персоналу з метою уникнення випадків порушення ІБ внаслідок незнання правил чи відсутності необхідних навичок у працівників підприємства;

– формування організаційної прихильності шляхом засобів економічного стимулювання та мотивування, уникнення дисциплінарних методів.

Важливими технологічними умовами успішного ЗІБ є створення системи багаторівневого захисту, різноманіття захисних засобів та посилення найслабшої ланки [6].

1.2 Специфіка забезпечення інформаційної безпеки підприємства в умовах конкурентної боротьби

Сучасні особливості розвитку людства пов’язані з формуванням інформаційного суспільства, в якому фактично будь-яка діяльність людей здійснюється на основі використання послуг, що надаються за допомогою ІТ та технологій зв'язку.

Особливостями інформаційного суспільства, які мають ключове значення для розвитку усіх сфер життєдіяльності, зокрема і економічної, є збільшення ролі інформації, знань та ІТ; наростаюча інформатизація суспільства; створення глобального інформаційного простору, що забезпечує доступ до інформаційних ресурсів; розвиток електронної економіки і зокрема електронних комерції, банкінгу, електронних господарюючих мереж.

З огляду на це конкурентна боротьба між суб’єктами підприємництва переходить в інформаційну сферу і може мати такі стадії:

– стадія мирного співіснування, за якої однак виникають інформаційні конфлікти незначні за своїми масштабами, не здатні завдати помітної шкоди економічним відносинам і корпоративним інтересам кожного учасника конфлікту, а, отже грають швидше регулюючу роль у конкурентній боротьбі. Економічні суб’єкти таким чином виявляють виникаючі протиріччя на ранніх стадіях і своєчасно вживають заходи щодо їх усунення;

– стадія зіткнення інтересів, за якої виявлені суперечності можуть призвести до подальшого загострення відносин та ескалації конфлікту, збільшення його масштабів, інтенсивності, залучення до нього нових суб'єктів і сфер діяльності, появи протиріч, породжених самим процесом перебігу конфлікту. На цій стадії конфлікту взаємовідносини суб'єктів продовжують розвиватися за законами мирного співіснування, проте погасити цей конфлікт (або направити його в інше русло) можуть тільки скоординовані спільні зусилля його учасників;

– стадія конфронтації (загрозливий період), в яку конфлікт переростає при небажанні конкурентів іти на поступки і компроміси в принципових питаннях. В умовах конфронтації, як правило, зачіпаються корпоративні інтереси (в їх ключових аспектах) учасників конфлікту, вирішення конфлікту на умовах одного з учасників неминуче завдасть значної шкоди інтересам інших. На цій стадії повернення до мирного існування ще можливо як за взаємною згодою конфліктуючих сторін, так і під впливом зовнішнього регулюючого чинника - наприклад, держави чи арбітра;

– стадія війни - крайня форма вирішення конкурентних протиріч з використанням інформаційних засобів [13].

На сучасному етапі у ході конкурентної боротьби використовуються різні методи інформаційного впливу, які дозволяють вирішити такі завдання:

- перехоплення та розшифрування інформаційних потоків, що передаються різними каналами зв'язку, або використання спеціальних технічних засобів для перехоплення інформації з метою отримання розвідувальної інформації, яку неможливо отримати офіційним шляхом;

- перехоплення та обробка відкритої інформації, що передається незахищеними каналами зв'язку, циркулює в інформаційних системах чи опублікована у відкритих джерелах та ЗМІ для отримання необхідних даних;

- технічний вплив на елементи ІТКС противника;

- психологічний вплив, спрямований на персонал та осіб, що приймають рішення;

- формування і масоване розповсюдження через інформаційні канали та глобальні мережі інформації, вигідної ініціатору, дезінформації, чуток;

- несанкціонований доступ до інформаційних ресурсів конкурента;

- захист від аналогічних впливів з боку конкурента [14].

Конкуренція є боротьбою між бізнес-конкурентами за найбільш вигідні умови виробництва і збуту продукції чи послуг. Історичний досвід показує, що загалом конкуренція сприяє розвитку продуктивних сил і прогресу суспільних відносин, проте лише тоді, коли вона має цивілізовані форми. Вважається, що саме в цьому разі перевагу отримує той суперник, чия стратегія спрямована на підвищення якості пропонованих товарів і послуг, зниження цін на них, надання додаткових пільг споживачам. В протиборстві між конкурентами також можуть застосовуватись і нецивілізовані, недобросовісні і навіть незаконні засоби та методи [15].

У сучасних уявленнях про ІБ бізнесу переважає бачення, відповідно до якого основним змістом ЗІБ підприємства є захист інформації, зокрема запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації; несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації; збереження конфіденційності документованої інформації відповідно до законодавства тощо.

Однак, слід звернути увагу на багатофункціональність інформації, яка проявляється у підприємницькій діяльності. Очевидно, що інформація є основою знань, тобто інтелектуального потенціалу суб’єктів підприємництва і які безумовно необхідно захищати. Водночас інформація є умовою ефективного здійснення підприємницької діяльності, вона використовується як засіб впливу на ринкову ситуацію, взаємовідносини суб’єктів, інформація має комерційну цінність і може виступати окремим видом економічної діяльності.

Так, на думку окремих авторів, ототожнення ЗІБ лише з захистом інформації при такій різноманітності її властивостей і функцій не є доцільним. ІБ крім захисту інформації суб’єкта підприємництва (інформаційних ресурсів та інфраструктури) передбачає інформаційне забезпечення підприємницької діяльності та протидію негативному інформаційно-психологічному впливу.

На основі використання зазначеного підходу під ЗІБ підприємства можна розуміти діяльність суб’єктів підприємництва щодо ефективного інформаційного супроводу бізнес-діяльності, надійного захисту інформаційних

ресурсів та інфраструктури підприємства і результативна протидія негативному інформаційно-психологічному впливу [16].

Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту ІБ забезпечує суб'єктам підприємництва необхідний рівень живучості у їх конкурентній боротьбі, оптимальну поведінку у взаємовідносинах з конкурентами, зацікавленими організаціями та інституціями, громадськістю.

Метою ЗІБ у такому випадку є виключення можливості втрати суб'єктами підприємництва своїх інформаційних ресурсів чи їх руйнування, заподіяння шкоди іміджу компанії, а також формування інформаційних передумов для ефективної діяльності і отримання прибутку. Критерієм же ефективності ІБ є стабільність позиції суб'єктів підприємництва на ринку та позитивні перспективи їх розвитку.

На думку фахівців, досягнення визначеної мети ЗІБ має забезпечуватись виконанням таких завдань:

- організація відповідного режиму функціонування інформації в діяльності суб'єктів підприємництва;
- формування, необхідних для забезпечення ефективної діяльності суб'єктів підприємництва, інформаційних ресурсів;
- своєчасне виявлення загроз інформаційним ресурсам та іміджу суб'єктів підприємництва, їх інформаційним відносинам;
- оперативне реагування суб'єктів підприємництва на зміни та порушення умов інформаційних відносин, спроби посягань на їх інформаційні ресурси та імідж;
- забезпечення інформаційного впливу в необхідних суб'єктам підприємництва сегментах ринку;
- підготовка персоналу суб'єктів підприємництва з питань їх ІБ;
- оптимізація заходів та витрат пов'язаних із ЗІБ підприємницької діяльності [16].

Зазначені завдання мають бути інтегровані у повсякденну діяльність суб'єктів підприємництва шляхом планової роботи як спеціальних підрозділів ІБ, так і всіх інших, що входять до складу організаційної структури суб'єктів.

Останні мають забезпечувати свою ІБ всією сукупністю своїх економічних, інтелектуальних, технічних, кадрових можливостей.

Основними принципами тут виступають:

- *законність* – заходи, що здійснюються в межах організації та ЗІБ, мають вкладатися в межі чинного законодавства, не порушувати прав та свобод громадян, законних інтересів інших суб'єктів та держави;
- *самостійність та відповідальність* – заходи ЗІБ обираються суб'єктами підприємництва самостійно, в межах своїх можливостей і повинні бути адекватними загрозам їх ІБ; за результати вжитих заходів відповідальність покладається на суб'єктів підприємництва та уповноважених ними на проведення таких заходів осіб;
- *компетентність* – виконання заходів ЗІБ має здійснюватися грамотно, на високому професійному рівні, підготовленими для цього фахівцями;
- *економічна доцільність* – витрати на організацію та виконання заходів ЗІБ повинні бути адекватними її ефективності, не завдавати шкоди економічному стану суб'єктів підприємництва;
- *цілеспрямованість* – заходи ЗІБ мають здійснюватися у строгій відповідності основним завданням і напрямам діяльності суб'єктів підприємництва;
- *конфіденційність* – переважна сукупність заходів ЗІБ проводиться на конфіденційній основі, інформування про їх проведення та результати здійснюється лише обмеженому колу осіб.

Надійність та ефективність ЗІБ суб'єктів підприємництва визначається через його відповідність встановленим вимогам, якими можуть бути:

- *безперервність ЗІБ* – заходи ЗІБ проводяться з початком її організації і продовжуються протягом всього часу існування суб'єкта підприємництва, посилюючись та послаблюючись в окремих ситуаціях, але без їх припинення;
- *плановість ЗІБ* – встановлення відповідного порядку застосування заходів ЗІБ, який має забезпечувати запобіжний характер їх впливу на потенційні ризики і загрози;

- *конкретність ІБ* – заходами ЗІБ мають бути охоплені конкретні об’єкти та дії суб’єктів підприємництва; заходи безпеки повинні бути пов’язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час суб’єктами підприємництва;
- *активність ЗІБ* – в арсеналі заходів ЗІБ повинні бути як такі, що забезпечують захист інформаційних ресурсів та іміджу суб’єктів підприємництва, інформаційно-аналітичний супровід бізнес-діяльності, так і ті, що спрямовуються на протидію негативним впливам та розкриття їх джерел;
- *комплексність ЗІБ* – передбачає необхідність застосування у забезпеченні безпеки різних форм, методів, засобів, заходів щодо різних видів інформації та інформаційних відносин [16].

Реалізація принципів і вимог до ЗІБ неможлива без конкретизації самого об’єкта ІБ. Враховуючи багатофункціональність інформації можна виявити її наявність у будь-якому матеріальному чи нематеріальному об’єкті або будь-якому виді діяльності. Тобто, будь-який об’єкт чи діяльність можна подати через призму інформації, зробити уявлення про нього на основі його інформаційних характеристик.

Інформація про щось може бути об’єктом ЗІБ лише тоді, коли вона буде мати певну цінність (для підприємництва – комерційну цінність) і щодо неї буде проявлена зацікавленість з боку інших осіб. Враховуючи наведене, інформацію як об’єкт ЗІБ можна подати таким чином (Рис. 1.5.).

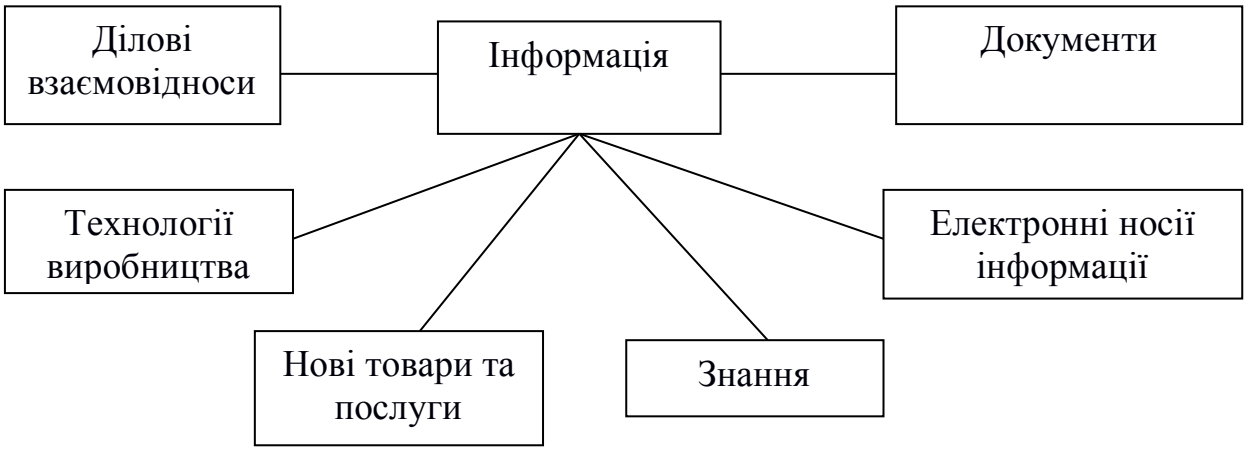

Рис. 1.5. Інформація як об’єкт ЗІБ.

На думку фахівців [16], аналізуючи практику інформаційних відносин суб’єктів підприємницької діяльності та беручи до уваги роль інформації в такій

діяльності, можна говорити, що ІБ підприємництва включає такі аспекти: інформаційно-телекомунікаційний, інформаційно-психологічний та документаційний.

Інформаційно-телекомунікаційний аспект ЗІБ передбачає: захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях або передається засобами ІТКС; отримання необхідної суб'єктам підприємництва інформації із глобального інформаційного простору (мережі Інтернет) для формування їхніх інформаційних ресурсів; протидія інформаційним загрозам в кіберсередовищі (комп'ютерні віруси, шкідливі програми, комп'ютерний тероризм тощо), а також захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок).

Інформаційно-психологічний аспект ЗІБ підприємства зосереджує свої зусилля у сфері інформації-знань та їх носіїв (працівників, клієнтів, споживачів продукції суб'єктів підприємництва). Основними напрямами забезпечення інформаційно-психологічної безпеки є захист інформації-знань (організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин); розробка технологій отримання знань (наукові дослідження, конференції, семінари, курси, симпозіуми тощо) для формування інформаційних ресурсів суб'єктів підприємництва; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Також до інформаційно-психологічного блоку ЗІБ підприємства варто віднести проведення заходів пропаганди, контрпропаганди та агітації в інформаційному середовищі суб'єктів підприємництва; протидія поширенню негативної інформації засобами масової комунікації.

Документаційне забезпечення ІБ спрямоване перш за все на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань ІБ; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, публікацій тощо) для формування інформаційних ресурсів суб'єктів підприємництва.

Водночас, на нашу думку, в сучасних умовах окремою і не менш важливою складовою ЗІБ підприємства є інформаційно-аналітична діяльність.

Таким чином, основними складовими ЗІБ підприємства можна вважати:

– інформаційно-телекомунікаційний (захист ІТКС),

– інформаційно-психологічний (захист та протидія деструктивним інформаційно-психологічним впливам),

– документаційний (формування та захист інформаційних ресурсів) та

– інформаційно-аналітичний (збір та обробка інформації) (Рис.1.6.)

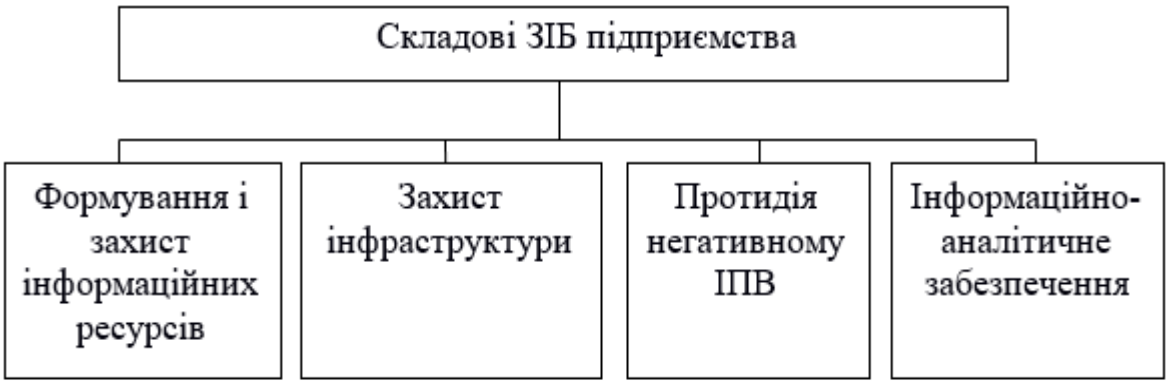

Рис.1.6. Аспекти ЗІБ підприємства.

Розглянемо сутність інформаційно-аналітичного блоку ЗІБ підприємства. Отже, інформаційно-аналітична робота (далі - ІАР) - це діяльність пов’язана зі збором і обробкою відкритої інформації, формуванням відповідних інформаційних документів та наданням їх керівництву суб’єкта підприємництва. Тобто ІАР - це насамперед діяльність в середовищі відкритої інформації, причому діяльність пов’язана зі збором інформації, її обробкою та формуванням відповідних інформаційних документів. Кінцевим етапом ІАР є інформування керівництва суб’єктів підприємництва. Варто відзначити, що в науковій літературі часто відносять до ІАР також і інформаційно-пошукову діяльність.

Основним в організації ІАР є визначення сфер інформаційної уваги, об’єктів і джерел інформації, оскільки це дозволяє краще конкретизувати і спрямувати дану роботу, сконцентрувати зусилля суб’єктів підприємництва на найбільш важливих її напрямках. Справа в тому, що інформаційне середовище підприємницької діяльності є досить значним, неоднорідним, обсяги інформації в ньому є такими, що не дають можливості без ефективної організаційної роботи

здійснювати інформаційне забезпечення суб'єктів підприємництва. За таких умов зазначені суб'єкти змушені сегментувати сфери інформаційного середовища, де у подальшому будуть виконувати необхідну їм інформаційну діяльність [17].

Таким чином, сфера інформаційної уваги суб'єкта підприємництва - це сегмент інформаційного середовища, в якому він забезпечує стратегічні, тактичні та оперативні інформаційні інтереси і завдання.

Враховуючи специфіку діяльності суб'єктів підприємництва та структуру їх інформаційного середовища, сфера інформаційної уваги включає:

– сферу інтересів, яка може бути представлена інформацією про об'єкти, регіони, галузі економіки, до яких прагне проникнути суб'єкт у майбутньому, події, які характеризують відповідні ринки;

– сферу впливу, яка характеризується інформацією про події, об'єкти, що можуть здійснювати вплив на поточну діяльність суб'єкта;

– сферу безпосередньої діяльності - інформацію про об'єкти та події, які характеризують або впливають на проведення тієї чи іншої операції, що здійснюється суб'єктом на даний час.

Як правило, суб'єкти підприємництва забезпечують роботу у всіх сферах інформаційної уваги і використовують інформацію: сфери інтересів - як стратегічну для прийняття рішень щодо довгострокових угод, договорів, планування перспектив розвитку; сфери впливу - як тактичну для прийняття рішень щодо співробітництва з партнерами, інвестування (вкладання) коштів в нові проекти, протидії недобросовісній конкуренції, визначення поведінки на ринку в той чи інший період часу; сфери безпосередньої інформаційної діяльності - як оперативну для прийняття рішень щодо безпосереднього здійснення конкретної операції, укладання конкретної угоди [16].

Основними факторами, які безпосередньо обумовлюють визначення сфер інформаційної уваги можуть бути: сфери і галузі економіки, бізнесу, в яких здійснює свою діяльність компанія, плани його розвитку; стан конкуренції на ринку, агресивність конкурентної боротьби, наявність, види, небезпечність загроз діяльності суб'єкта та особливості поточної діяльності; необхідність формування (підтримання) позитивного іміджу суб'єкта в його інформаційному середовищі; інтереси суб'єкта та особливості його поведінки на ринку.

Висновки до першого розділу

У результаті дослідження встановлено, що ЗІБ підприємства має на меті створення умов для збереження цілісності, повноти й точності інформації, мінімізація ризику несанкціонованих змін у корпоративних ІТКС.

ЗІБ підприємства включає широкий спектр різнопланових заходів, які можна класифікувати, зокрема, за орієнтацією на об’єкти (персонал, матеріальні і фінансові цінності, інформаційні ресурси), способами дій (запобігання, виявлення, припинення і відновлення), охопленням (територія, приміщення, технічні та програмні засоби, носії інформації, персонал) тощо.

Аналіз наукових джерел показав, що систему ЗІБ підприємства можна визначити як сукупність організаційних, нормативних, технічних, програмних заходів, які впроваджуються у контексті вимог бізнесу з метою гарантувати стан захищеності інтересів підприємства в інформаційній сфері.

З’ясовано, що сьогодні в умовах збільшення ролі інформації та ІТ в організації успішного функціонування бізнесу загалом та забезпеченні ІБ підприємства, конкурентна боротьба між суб’єктами підприємництва переходить в інформаційну сферу. Передумовами таких тенденцій є також економічна вигідність, скритність та латентність дій в інформаційному просторі; використання різноманітних методів і засобів інформаційно-психологічного впливу.

Таким чином, в умовах гострої конкурентної боротьби змістом діяльності із ЗІБ підприємства стає не тільки захист інформаційних ресурсів та інфраструктури підприємства, запобігання несанкціонованим діям з інформацією та забезпечення її конфіденційності, але й інформаційне забезпечення підприємницької діяльності.

Розділ 2.
ОСНОВНІ ЗАСАДИ КОНКУРЕНТНОЇ РОЗВІДКИ

2.1 Сутність, цілі та етапи конкурентної розвідки

Як відзначалося вище, успішне ЗІБ сучасного підприємства є неможливим без здійснення цілеспрямованої, послідовної та кваліфікованої діяльності зі збору, обробки інформації з важливих питань життєдіяльності суб'єкта підприємництва та інформування керівництва з метою прийняття оптимальних управлінських рішень.

У нинішніх умовах основний перелік завдань з інформаційно-аналітичного ЗІБ підприємства виконує конкурентна розвідка. Розглянемо сутність поняття «конкурентна розвідка» у контексті різних підходів.

Конкурентна розвідка – це координований та цілеспрямований моніторинг конкурентів, продуктів та клієнтів на певному ринку або у певній галузі. Ці дані використовуються менеджерами та виконавцями для прийняття кращих стратегічних рішень для організації [18]. Окрім цього, це важливий компонент для розробки бізнес-стратегії. Аналіз конкурентної розвідки забезпечує розуміння динаміки ринку та проблем структурованим, дисциплінованим та етичним способом, використовуючи опубліковані та не опубліковані джерела [19].

Конкурентна розвідка включає в себе вибір, збір, розуміння та розповсюдження стратегічної інформації, яка є загальнодоступною, і на відміну від промислового шпигунства, не передбачає крадіжку конфіденційної інформації. Як правило, залучає отримання інформації про зовнішнє конкурентне середовище, наприклад дані про попередні моделі у бізнесі конкурента. У свою чергу, промислове шпигунство передбачає використання неетичних методів отримання інсайдерської інформації [18].

Конкурентна розвідка може також означати різні речі для різних людей всередині організації. Наприклад, для торгового представника це може означати тактичні поради щодо того, як найкраще запропонувати вигідний контракт. Для топ-менеджменту це може означати унікальну маркетингову статистику, щоб отримати частку на ринку від великого конкурента.

Кінцевою метою конкурентної розвідки є допомога у прийнятті кращих

рішень та підвищення ефективності організації.

Водночас конкурентна розвідка є інструментом забезпеченння інформаційної безпеки підприємства шляхом інформаційно-аналічтиного забезпечення усіх бізнес-процесів.

Хоча більшість компаній можуть знайти суттєву інформацію про своїх конкурентів в Інтернеті, конкурентна розвідка виходить далеко за рамки простого трасування Інтернету, за умови, що найцінніша інформація рідко є легкодоступною. Типовий аналіз конкурентоспроможної інтелектуальної інформації включає дані та аналіз з численних джерел. До них відносяться засоби масової інформації, інтерв'ю з клієнтами, конкурентами та експертами галузі, виставки та конференції, громадські опитування тощо [20].

Конкурентна розвідка передбачає використання відкритих джерел для розробки даних про конкурентів, конкурентного та ринкового середовища. Потім, завдяки аналізу, перетворює ці дані в розвідку.

Фахівці конкурентної розвідки:

- ідентифікують інформацію, необхідну особі, що приймає рішення в конкурентному середовищі;
- збирають необроблені дані, використовуючи правові та етичні засоби, з загальнодоступних джерел;
- аналізують ці дані, використовуючи будь-який з найрізноманітніших інструментів, перетворюючи їх в розвідку, за якою передбачається вживання заходів;
- передають готову розвідку для тих, хто приймає рішення для використання.

В конкурентній розвідці “загальнодоступні джерела” – це вся інформація, яку можна етично та легально ідентифікувати, знайти, та отримати до неї доступ, тобто там, де розташовані первинні дані [21].

Метою конкурентної розвідки – є аналіз і систематизація чесно здобутої інформації.

Конкурентна розвідка – перш за все, маркетинговий інструмент вивчення конкурентного середовища, який є цілеспрямованим збором інформації про конкурентів для ухвалення управлінських рішень щодо подальшої стратегії та тактики ведення бізнесу [22]. З іншого боку, мета конкурентної розвідки полягає у ранньому визначенні можливостей у конкурентному середовищі,

перш ніж вони можуть стати очевидними для всіх інших, а також можливість знайти ризики, перш ніж вони завдадуть шкоди безпеці організації [18].

Цілі конкурентної розвідки:

- Надати завчасне попередження про ризики та можливості, такі як злиття, поглинання, альянси, нові продукти та послуги.
- Переконатися в тому, що стратегічне планування рішення, спирається на актуальну та сучасну конкурентну розвідку.
- Знайти спроможність організації для адаптування та реагування на зміну конкурентного середовища.
- Надати періодичний та систематичний аудит конкурентоспроможності фірми, який забезпечує об'єктивну оцінку фактичної позиції фірми щодо навколишнього середовища [23].

Загалом можна виділити такі інтегровані завдання конкуретної розвідки:

– забезпечення своєчасного інформаційно-аналітичного супроводу прийняття управлінських рішень. Це пов'язано з необхідністю вироблення своєчасних і обґрунтованих управлінських рішень як на стратегічному, так і на тактичному рівні;

– своєчасне залучення уваги осіб, які приймають управлінські рішення в організації, до загроз, що можуть заподіяти шкоду бізнесу;

– виявлення сприятливих можливостей для бізнесу;

– уникнення ділових відносин з несумлінними або залученими до кримінальної діяльності партнерами; запобігання загрозливим діям з боку конкурентів, співробітників або регуляторів ринку;

– недопущення (спільно зі службою безпеки) спроб конкурентів отримати доступ до закритої, конфіденційної інформації організації;

– проектування механізму управління ризиками. Ця інформація дозволяє підприємству ефективно реагувати на швидкі зміни навколишнього середовища [24]. (Рис. 2.1.)

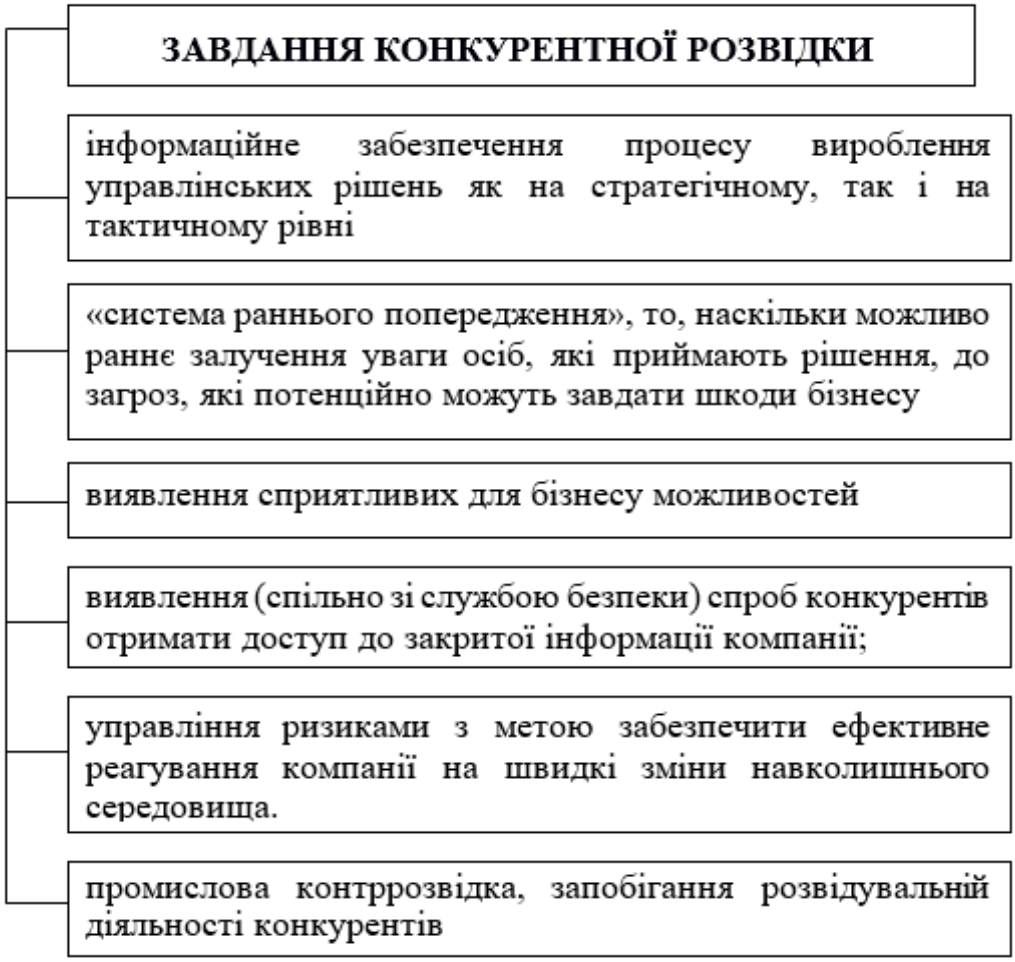

Рис. 2.1. Завдання конкурентної розвідки

Процес конкурентної розвідки, як правило, формально розподіляється професіоналами на п'ять основних етапів, кожний з яких пов'язаний один з іншими за допомогою циклу зворотного зв'язку. Ці фази, що складають спеціалісти конкурентної розвідки, називають цикл конкурентної розвідки (рис 2.2):

1) Складання потреб конкурентної розвідки. Це визначення необхідності потреб конкурентної розвідки та визначення того, який тип конкурентної розвідки потрібен кінцевому користувачеві. Це тягне за собою розгляд проблеми, які запитання є мотивацією завдання та на які запитання кінцевий користувач хоче відповісти за допомогою конкурентної розвідки. А також, хто ще може також використовувати конкурентну розвідку, і як, ким і коли вона, зрештою, буде використана;

2) Збір початкових даних. Спеціаліст конкурентної розвідки перетворює потреби кінцевого користувача в план дій, формально чи неофіційно. Це, як правило, ідентифікує запитання, які потребують відповіді, і тоді, цілком

імовірно, що він може зібрати дані, необхідні для створення відповідей на ці запитання. Спеціаліст конкурентної розвідки повинен мати реалістичне розуміння всіх суттєвих обмежень, таких як часове, фінансове, організаційне, інформаційне та правове. Тоді він може визначити оптимальні джерела даних, тобто ті, які, найімовірніше, дадуть достовірні та корисні дані, враховуючи мету та вимоги. Звідси розпочинається збір, як вторинних, так і первинних даних;

3) Оцінка та аналіз початкових даних. На цьому етапі зібрані дані оцінюються, аналізуються та перетворюються у вигідну конкурентну розвідку. Це може бути зроблено особою, яка виконує це сукупно, або окремими аналітиками. Існує два способи, в яких аналіз розповсюджується на весь процес. Перший – це використання аналізу, щоб зробити вибір, наприклад, вирішувати, які із десятків новинних статей найважливіші для читання та вивчення. Другий – використання аналізу для додавання одного або декількох елементів даних. Наприклад, додавання заяви до короткого звіту, вказуючи, чому і як його вміст важливий для кінцевого користувача;

4) Передача обробленої інформації. Передбачає підготовку, а потім представлення результатів у практичному форматі та своєчасно;

5) Вжиття заходів. Це означає, що використання кінцевого користувача насправді використовує розвідку для прийняття рішень. Конкурентна розвідка може використовуватися як допомога для прийняття рішень, або це може бути першим з кількох кроків загальної оцінки, наприклад, нового ринку. Рішення про те, як і коли це використовується, здійснюється кінцевим користувачем, а не аналітиком [19].

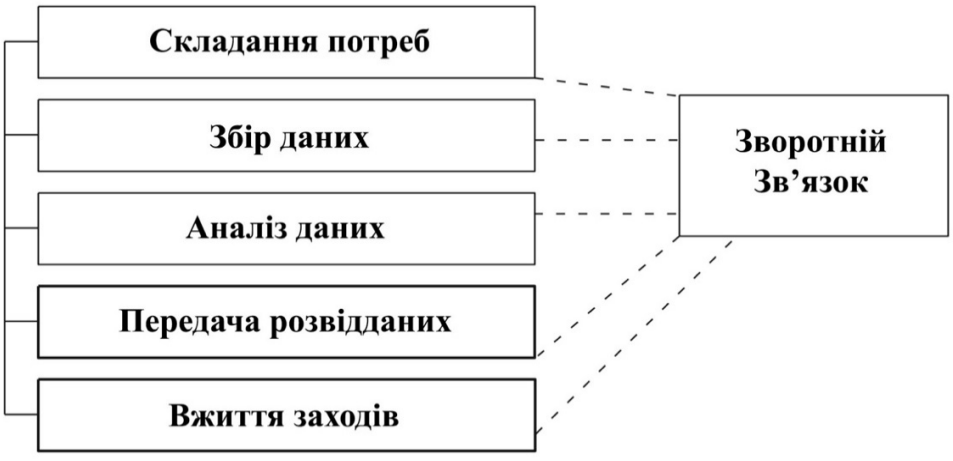

Рис. 2.2. Цикл конкурентної розвідки

Як правило, політика конкурентної розвідки повинна відповідати чотирьом

основним принципам:

1. Автентичність. Автор вважає, що збираючи дані, не треба використовувати чужу ідентифікаційну інформацію. Наприклад, якщо підписатися на отримання маркетингових електронних повідомлень від конкурента, то слід використовувати офіційну адресу компанії. Якщо постане питання від конкурента, правильною буде відповідь, що причиною підписки служить "оцінка продукту або послуги".

2. Дотримання всіх формальних угод. В ході збору інформації про конкурентів, можуть забезпечуватися джерела, пов'язані з галуззю або конкретним конкурентом. За словами автора, необхідно перевірити та впевнитися, що такі джерела не сприяються, навіть випадково. Таким чином можуть порушитися будь-які постійно діючі домовленості чи угоди.

3. Дотримання всіх прав та законів інтелектуальної власності. Як відомо, технічні аспекти права інтелектуальної власності є складними, що надалі може легко привести до конфлікту. При отриманні доступу чи вивченні продуктів або послуг інших компаній, автор радить ретельно проконсультуватися з адвокатом, перш ніж використовувати засновані знання на практиці.

4. Пильний моніторинг консультантів. Коли справа доходить до конкурентної розвідки, ахіллесова п'ята багатьох компаній – це не їхні співробітники, а сторонні консультанти. При залученні третіх осіб для будь-яких цілей, автор вважає, варто переконатися, що вони знають і дотримуються політики організації, яка їх і залучила [25].

Оскільки інформація відіграє ключову роль у розвідувальній діяльності, розглянемо основні види та джерела розвідувальної інформації.

Інформацію прийнято вважати цінною лише тоді, коли її можна використовувати, причому корисність інформації дуже залежить від її повноти, точності і своєчасності.

Слід конкретно розрізняти і не плутати: факти (дані), думки (особистісні припущення), інформацію (аналітично оброблені дані).

Всі джерела інформації про зовнішнє оточення фірми можна класифікувати за різними підставами:

1. за ступенем відкритості (закриті, умовно відкриті і відкриті);

2. по відношенню до компанії дослідника (внутрішні і зовнішні);

3. за суб'єктами (джерела органів влади та місцевого самоврядування,

некомерційних організацій, комерційних організацій, приватних осіб);

4. за унікальністю (оригінали, копії), витяги, фрагменти, запозичення);

5. за фізичною природою (люди, речі та документи).

Закриті джерела і носії інформації захищені законами про державну таємницю, комерційну таємницю, персональні дані та іншими чинними нормативними актами. Очевидно, що збір, зберігання, обробка та розповсюдження інформації, отриманої з закритих джерел або носіїв, мають наслідком конфлікт із законом. Водночас, конфіденційну інформацію вдається отримувати з досить різноманітних джерел, більшу частину яких недосвідчена людина просто не бере до уваги.

Умовно відкритими вважають джерела і носії, доступ до яких не заборонений законодавством, але вимагає наявності спеціальних умов: навченого персоналу, грошових коштів для доступа до даних тощо.

Нарешті, відкритими джерелами і носіями інформації вважають ті, доступ до яких не заборонений законодавством і не вимагає особливих умов.

Відповідно до різних підходів інформація поділяється на:

- тотальну (дає загальне оглядове уявлення про проблему, що цікавить, учасників-індивідів і організації);
- поточну або оперативну (тримає в курсі подій, що змінюються);
- конкретну (заповнює виявлені прогалини в даних або відповідає на певні питання);
- непряму (підтверджує або спростовує певні припущення, що стикуються з останніми тільки опосередковано);
- оцінкову (пояснює події і дає прогноз щодо їх розвитку в майбутньому; це – оптимально оброблені дані) [26].

2.2 Логіка процесу дослідження та методи конкурентної розвідки

Логіка процесу дослідження.

Конкурентне середовище як своєрідну, цілісну та самостійну систему функціонування бізнесу ділять на дві складові: предмет і метод. Якщо предмет – це чітко визначений зміст, якість та закономірність, в яких реальність (дійсність) постає перед дослідником, то метод – це шлях осягнення суті предмета пізнання. Метод можна також визначити як сукупність прийомів і

способів емпіричного та теоретичного пізнання. Виникнення нової галузі наукового знання завжди пов’язане зі змістовою диференціацією уявлень людини про світ (об’єктивним процесом розвитку науки), виділенням сутнісно нового змісту в існуванні досліджуваної реальності (визначенням предмета) та побудовою засобів пізнання цієї реальності (створенням методу).

Методику розуміють як сукупність прийомів дослідження, включаючи техніку й різноманітні операції з фактичним матеріалом.

Методика дослідження – це сукупність принципів, способів та методів, за допомогою яких буде вирішена проблема дослідження.

Методика конкурентної розвідки – послідовність конкретних процедур, реалізація яких забезпечує досягнення мети бізнесу. При цьому процедура – це встановлений порядок виконання прийомів та способів дослідження.

Прийом розглядається як певна дія для досягнення мети дослідження, а спосіб – система дій, які здійснюються під час певного дослідження.

Методика дослідження при вирішенні конкретної проблеми чи завдання має сталу структуру, основними елементами якої є:

1) теоретико-методологічна частина, на основі якої конкурента розвідка розглядається як самостійна складова системи економічної безпеки;

2) історико-теоретична, що передбачає дослідження явищ, процесів з урахуванням зв’язків та взаємозалежностей між ними. Так, формування конкурентної розвідки на підприємстві неможливе без попереднього діагностування етапів розвитку компанії, намірів на перспективу, наявної інформації тощо;

3) практична, тобто узагальнення результатів дослідження як логічне завершення інформаційного пошуку, їх аргументація.

Підґрунтям застосування відповідних процедур у бізнесі повинні бути принципи, на яких ґрунтується вся діяльність конкурентної розвідки. Принцип за своєю суттю є початком, базою, він лежить в основі певної сукупності фактів, теорій, наук. Беззаперечним є той факт, що будь-яка теоретична система знань ґрунтується на взаємопов’язаних принципах.

Варто розглянути ті принципи, які повинні складати основу застосування різних підходів у процесі конкурентної розвідки.

Із метою уникнення однобічності діяльності конкурентної розвідки її діяльність повинна ґрунтуватись на застосуванні принципу взаємозв’язку

системи із зовнішнім середовищем. Його суть зводиться до того, що досліджуючи зовнішнє та внутрішнє середовище компанії, конкурентна розвідка повинна враховувати всі суттєві взаємозв'язки з іншими напрямами забезпечення безпеки бізнесу: юридичним, технічним, організаційним.

Наступний принцип, який посідає особливе в місце роботі конкурентної розвідки є принцип об'єктивності. Результати діяльності конкурентної розвідки, передусім, повинні бути об'єктивними. Якщо компанії загрожує крах, про це треба доповісти, інакше він точно настане.

Важливий принцип, який дає змогу підсилити теоретичні висновки практичними прикладами є принцип єдності теорії та практики. Так, у роботі конкурентної розвідки потрібно постійно проводити різні тренінги, навчальні семінари, підвищувати кваліфікацію її співробітників.

Загальним принципом, який притаманний всім напрямам діяльності компанії є принцип розвитку. Будь-яка діяльність компанії, зокрема конкурентна розвідка, повинна вносити щось нове в бізнес і в такий спосіб забезпечувати стабільний прогрес його розвитку.

Для логічного застосування різних методів конкурентної розвідки використовуються певні наукові підходи. Підхід розуміється як спосіб організації принципів та методів дослідження.

Основу всіх підходів становить методологія роботи конкурентної розвідки. Методологія розглядає теоретичні проблеми пізнання та закономірності їх дослідження як творчого процесу.

Методологія в широкому розумінні – це вчення про структуру, логічну організацію, методи та засоби діяльності.

Методологія – це вчення про загальні точки зору, на які повинен зважати дослідник. Оскільки ці точки зору, правила та засоби не довільні, а визначені однією кінцевою метою – пізнати предмет таким, яким він є насправді, тобто дослідити теоретико-методологічні засади, організаційні та правові основи, напрями стратегічного управління.

Оскільки будь-яка методологія ґрунтується на своєрідності предмета та передбачає попереднє пізнання його загальних, формальних властивостей, саме тих властивостей, від яких залежать правила, прийоми та підходи, можна назвати функції методології конкурентної розвідки:

- визначає способи здобуття нових знань, які відображають динамічні

процеси та явища, що стосуються інформаційного середовища компанії;

- направляє, передбачає особливий шлях, на якому досягається теоретичне обґрунтування й системне розроблення теоретико-методологічних основ та емпірично-методичних засобів комплексного дослідження й визначення конкурентної розвідки як пріоритетного напряму розвитку бізнесу;

- забезпечує всебічність отримання інформації щодо практики конкурентної розвідки та можливих шляхів її вдосконалення спираючись на міжнародний досвід;

- забезпечує уточнення, збагачення, систематизацію термінів і понять;

- створює систему інформації, яка базується на об’єктивних фактах, і логіко-аналітичний інструмент пізнання [1].

Емпіричний рівень досліджень відноситься до отримання та обробки початкових фактичних даних. Він, як правило, ділиться на актуальні операції та наукові факти.

Актуальні операційні факти – це події, які мають своє місце у даний час, а також різні сторони або властивості, взаємозв'язок тестованих об'єктів.

Наукові докази – факти, представлені для розгляду в аналізі, зрозумілі та записані у формі логічної розвідки (дослідження).

Аналіз літератури показав, що методичне походження у дослідженні є основною ідеєю, яка поєднує в собі всі методи структурних елементів, і визначає організацію процедури і її фази.

Всі витоки методу мають свою власну логічну послідовність:

- Цілі, завдання, гіпотеза дослідження;

- Критерії, специфічні показники розвитку явища безпосередньо пов'язані з конкретними методологіями дослідження;

- Визначення послідовності використовуваних методів, процедури управління експериментом, процедури реєстрації, варіації та підсумовування експериментального матеріалу.

Методологія дослідження вибирається в залежності від цілей і завдань, поставлених для професіоналів конкурентної розвідки [1].

Методи аналізу загальнодоступних інформаційних джерел

З’ясовано, що під час роботи з загальнодоступною інформацією необхідно визначити цілі та завдання конкурентної розвідки та з'ясувати потреби клієнта, тобто інформацію, яку очікує споживач, і лише потім розпочати вибір джерел

інформації. Дуже важливо відрізнити інформацію, яка допомагає вирішити конкретні проблеми серед загального потоку загальнодоступної інформації. Для цього потрібні цільові інформаційні потоки. Це означає не збирати всю інформацію з загальнодоступних джерел у інформаційному просторі, а лише те, що може допомогти досягти поставлених цілей.

Для досягнення поставлених цілей необхідно розрізняти ключові слова, які допомагають підбирати відповідні джерела інформації. Фахівці стверджують, що для цього буде достатньо півгодини за умови, що аналітик конкурентної розвіки матиме відповідні навички роботи з такою методологією.

Наступним кроком буде збір інформації, потім класифікація, а потім остаточна стадія – збереження обраної інформації.

Також відомо, що дані, отримані з різних джерел інформації, дублюють один одного, що погіршує роботу спеціаліста конкурентної розвідки, не даючи бажаних результатів. Дане припущення полягає в тому, що аналіз інформаційного потоку у 7 мільйонів слів повинен поміститися в підсумковий звіт на 1-2 сторінки.

У майстерність спеціаліста конкурентної розвідки входить: здатність відрізняти релевантну інформацію від потоку інформації та помічати ідеї, що випливають з контексту. Хоча є ствердження, що публікації можна виділити як основу для підготовки базових звітів, але існують побоювання, що всі джерела інформації можуть бути заздалегідь передбачені, що може цікавим для інформаційного замовника.

Існує два напрями практичного використання:

- використання особистого потенціалу під час спілкування з громадськими ЗМІ;
- використання зовнішніх варіантів під час спілкування з громадськими ЗМІ.

Використання особистого потенціалу під час спілкування з громадськими ЗМІ. У цьому випадку відповідальна особа кожен день перебуває на так званій щоранковій "оперативній зустрічі" та представляє керівникам короткий огляд або звіт загальнодоступної інформації. До кожної слід додати список проблем, щодо яких експерти з питань розвідки повинні відповідати протягом дня, використовуючи інші джерела інформації. Вся інформація, надана на зустрічі, а також сирі джерела інформації, які представляють інтерес, повинні зберігатися в електронних базах даних, в яких можна знайти потрібну інформацію за

допомогою ключових слів.

Використання зовнішніх варіантів під час спілкування з громадськими ЗМІ. Інколи дешевше купувати оригінальну інформацію з інших джерел, включаючи спеціалізовані компанії. Проте, через відсутність контролю первинного джерела існує ризик втратити важливу інформацію; в цьому випадку постійна співпраця з конкретним підприємством є більш цілеспрямованою. Однак у цьому випадку існує ризик витоку інформації, оскільки іншій компанії стає відомо про інтереси бізнес-організації.

Існують випадки, коли спеціалісти відбираються для роботи на тимчасових контрактах. В цьому випадку вони, як правило, не знають, якою є мета збирання та яка інформація буде використовуватися.

Дослідження іноземних авторів показують, що первинна інформація, як у формі, так і в змісті, може відображати інтереси власників ЗМІ, тому ці дані повинні враховуватися спеціалістами з розвідки та бути показані у відповідних висновках. Також необхідна перевірка автентичності у додаткових джерелах інформації [27].

Методи конкурентної розвідки

Спеціалісти конкурентної розвідки виділяють деякі методи, які вони вважають легко пристосованими до потреб організацій. Вони стверджують, що немає абсолютно універсального прийому, і спеціалісти розвідки повинні використовувати різні методи залежно від характеру завдань.

Метод альтернативних ресурсів пропонує кілька пояснень для проблем конкурентної розвідки. Він використовується, коли спеціаліст конкурентної розвідки отримує суперечливі або неоднозначні дані з різних інформаційних джерел, а також, якщо, зрештою, користувач вимагає розглянути кілька можливих сценаріїв.

Метод аналізу можливості дозволяє спеціалісту конкурентної розвідки представити себе керівником, який повинен приймати рішення та передбачати можливі дії організації. Цей метод дозволяє визначити та оцінити потенційні ризики на безпеку підприємства, відповідаючи на запитання “Як ми повинні діяти?”. У цьому методі першим кроком буде переформування вирішення проблеми конкурентної розвідки на мову менеджера з прийняття рішень. Подальше застосування цього методу залежить від конкретної ситуації.

Контр-аналітичний метод має на меті замінити або відмовитися від

початкових припущень про конкурентів і переглянути напрями аналізу. Цей метод корисний, оскільки він ставить під сумнів чітку інформацію, щоб уникнути стереотипів та інших наслідків, що знижують якість аналізу. Цей метод дозволяє спеціалісту конкурентної розвідки послідовно переглянути всі можливі обґрунтування та варіанти дій конкурентів. Таким чином, цей метод допомагає аналітику уникнути вибору варіантів обмеженого розгляду.

Метод дивергенції характеризується безперервним посиленням гіпотези, поглядів чи ідей, що вимагають від спеціаліста розвідки бути уважним, творчим та стриманим. Використовуючи цю методологію, спеціаліст з питань конкурентної розвідки розробляє перелік припущень і розглядає, яким чином ці припущення можуть змінити підхід до проблеми. Пізніше він складає список запитань для збору даних і в кінцевому підсумку повторно визначає проблему. Гіпотеза повинна бути записана спочатку, тоді як потім аналітик конкурентної розвідки може випробувати три або більше гіпотезно-побудових методів, тобто теоретичний підхід, ситуаційний підхід та порівняльний підхід. Автор стверджує, що спеціаліст конкурентної розвідки повинен генерувати від 5 до 10 гіпотез і не менше 3, мотивуючи той факт, що менше трьох гіпотез рідко охоплюють всі бажані відповіді та варіанти вибору.

Метод фактичного аналізу містить ту чи іншу подію, що відбувається за межами середовища ділової організації, показує напрями розвитку, а також особливості дій конкурентів. Цей метод на якомусь рівні використовується всіма аналітиками, хоча не завжди точно дотримується методології. При використанні відповідно до негнучкої системи, цей метод може виявити важливі напрями розвитку у конкурентному середовищі організації. Таким чином, цей метод дозволяє заздалегідь виявити потенційні зміни у конкурентному середовищі. Проста хронологія дій конкурентів, аналіз останніх закупівель підприємства, географічні дані конкурентної діяльності тощо.

Метод аналізу конкурентних гіпотез дозволяє порівнювати результати та отримати пояснення дій конкурентів. Ця методологія забезпечує аналітиків конкурентної розвідки можливістю перевіряти сумісність даних, зібраних розвідкою, та визначити можливі неточності у остаточному звіті. Згодом ці дані додатково аналізуються. У більшості випадків спеціаліст вибирає одну гіпотезу, яка могла б підтвердити його думку та пояснити процес. Це продовжується до тих пір, поки не буде спростовано вибір цієї гіпотези. Недоліком такої ситуації є

те, що аналітик конкурентної розвідки, який оцінює гіпотези одну за одною, часто втрачає можливість порівнювати та оцінювати всі зібрані дані та кількість гіпотез одночасно. Таким чином з'являється можливість не тільки вибирати, яка гіпотеза краще заснована на зібраних даних, але одночасно перевірити інформаційні джерела первинних даних.

Таким чином, спеціаліст з питань конкурентної розвідки повинен мати можливість вибирати відповідну методологію, яка дозволяє проводити необхідний аналіз та отримати об'єктивні результати. Об'єктивність оцінок та успіхів безпосередньо залежить від цього [27].

Також додатково виділяють особисту розвідку конкурента. Аналіз ділових зв’язків і комунікативних контактів осіб, які приймають рішення. Безсумнівно, що бізнес роблять люди і інформація тільки про діяльність підприємства буде неповною для прийняття управлінських рішень. Тому для прояснення всіх загроз і можливих ризиків необхідна розвідка стосовно певної особи. Одержати таку інформацію можна за допомогою аналізу інформаційного поля: преса, інтернет. Щоб зменшити загрози, необхідно зрозуміти: яке коло ділових зв’язків одного з директорів компанії конкурента, які його психологічні риси, яка мотивація його дій, яку мету він собі ставить. Природно, що найбільш доцільним методом у цьому випадку буде опитування осіб, які володіють такою інформацією або є співробітниками цього підприємства.

Аналіз біографії керівників компанії конкурента. Це дасть масу відтінків для розуміння його психологічного портрета й допомагає визначити ймовірне коло його спілкування.

Аналіз ділового життя керівників компанії конкурента в позаробочий час. Це допоможе зрозуміти ступінь добропорядності конкурента.

Отже, порівнявши результати аналізу інформації про підприємство з результатами аналізу щодо персони, буде надана досить повна картина для формування власної думки про потенційні загрози безпеці підприємства [10].

Методи ідентифікації проблем

Спеціаліст з аналізу конкурентної розвідки з великомасштабним чи неспецифічним завданням може спричинити ситуацію, коли кількість можливих відповідей у результаті роботи може не задовольнити інформаційного замовника та може призвести до неточностей. Тут досвідчений аналітик конкурентної розвідки має вміти розробляти конкретні питання, які допоможуть прояснити

інформаційні потреби замовника (див. табл. 2.1.).

У цьому випадку проблеми згруповані, і кожна з них аналізується в декількох аспектах. На думку авторів, цей метод повинен допомогти визначити та оцінити проблеми, а також підготувати їх до подальшого аналізу.

Навідні запитання вимагають лише одну відповідь у кінцевому результаті. Робота спеціаліста конкурентної розвідки полягає в тому, щоб знайти відповідь або знати, де її знайти.

Висока ймовірність виникнення випадкових проблем характеризується тим фактом, що спеціаліст з аналізу конкурентної розвідки не знає і не може визначити всі можливі варіанти. Невизначені проблеми характеризуються тим, що питання і дані неповні та неточні [27].

Таблиця 2.1.

Методи ідентифікації проблем конкурентної розвідки

Характеристика	**Навідне запитання**	**Проблеми у невизначеному часі**	**Можливі непередбачені проблеми**	**Висока вірогідність випадковості**	**Не визначено / Не визначені**
Яке питання?	Збір інформації	Кількість	Оцінка всіх результатів	Оцінка результатів в умовах невизначеності	Передбачення майбутніх дій
Факти	Підтверджені	Частково підтверджені	Слабко підтверджені	Майже не підтверджені	Не підтверджені
Роль рішення	Абсолютно незначна	Незначна	Імовірно незначна	Значна	Дуже значна
Аналітичне завдання	Пошук інформації	Метод вибору	Підсумки результатів	Опис результатів	Опис факторів та перспектив
Аналітичний метод	Пошук джерела	Координація даних та методів	Аналіз корисності	Рольові показники	Моделювання аналізу

Продовження таблиці 2.1.

Інструменти аналізу конкурентної розвідки	Координація	Математична формула	Ймовірність корисності, діаграми впливу	Оцінка різних результатів	Експертна оцінка
Висновки аналізу конкурентної розвідки	Факти	Коментарі й обґрунтування	Альтернативний результат	Можливі результати	Підготовка в перспективі
Імовірність помилки	Низька	Дуже низька	Безпосередній зв'язок з достовірністю первинних даних	Велика	Найвеличезніша
Продовження діяльності конкурентної розвідки	Не передбачено	Не передбачено	Зміна спостереження	Повторний аналіз	Ретельний аналіз

Аналітичні методи конкурентної розвідки

Аналіз – це єдиний спосіб, за допомогою якого команда може по-справжньому витягнути цінну інформацію із зібраних даних, і мати шанс зіграти роль у процесі стратегічного планування компанії. Є багато методів аналізу конкурентного середовища, але варто виділити ті, які неодмінно впливають на структуру промисловості та конкурентоспроможність.

1. SWOT. Структурований метод аналізу як внутрішніх, так і зовнішніх чинників, які можуть вплинути на успіх компанії. Ця структура потребує незначного впровадження, оскільки вона використовується практично в кожному обговоренні стратегічного планування. Як зазначає автор, є застереження, що SWOT (Strengths, Weaknesses, Opportunities, Threats) може бути корисним для організації інформації, але, звичайно, не для керівництва у процесі прийняття стратегічних рішень. Щоб отримати додаткові статистичні дані, її потрібно поєднати з матрицею TOWS (Threats, Opportunities,

Weaknesses, Strengths).

2. Структура SCP. Основою SCP (Структура-Поведінка-Ефективність) є процес розуміння того, як поведінка конкурентів та зовнішні імпульси можуть вплинути на рентабельність та зростання майбутньої галузі. Часом буває важким для виконання, оскільки це вимагає, щоб керівники планували майбутні проекти, але тільки реальні ідеї, які б призвели до стратегічних дискусій.

3. ADL-матриця. Цей аналіз допомагає зрозуміти, як зрілість та конкурентоспроможність галузі впливають на стратегію. Він порівнює дві осі: галузь зрілості (починаючи від ембріональних, зростаючих, зрілих, і закінчуючи старіючими) та конкурентні позиції (від домінуючих до слабких).

4. П’ять сил Портера. Система Портера містить контрольний список для аналізу рівня конкурентоспроможності галузі на основі балансу сил. Проте це лише початок аналізу. Наступний крок включає визначення того, яка стратегія збільшить шанси на успіх: стратегія структури витрат, стратегія диференціації або стратегія інтеграції.

5. Промислові криві витрат. Використовуючи криві пропозиції, ця система допоможе прогнозувати потенціал інвестицій, закриття заводів та зміни цін на продукт.

6. Мережі створення цінності. Цей аналіз розширює структуру п'яти сил Портера, вивчаючи роль комплементарних компаній (компанії, у яких клієнти купують додаткові продукти або послуги) та їх вплив, що є дзеркальним зображенням конкурентів.

7. Просторова матриця. Це цінний спосіб аналізу конкурентної позиції організації. Він висвітлює два внутрішні виміри (фінансова сила та конкурентна перевага) та два зовнішні виміри (сила промисловості та стабільність у навколишньому середовищі) для визначення стратегічної позиції організації в галузі. Стратегічна сила компанії визначається як агресивна, конкурентоспроможна, консервативна або оборонна.

8. PEST. Ця структура використовується на ранніх етапах розробки стратегії для опису ландшафту та середовища, в якому працює фірма (PEST – політичний, економічний, соціальний та технологічний). Примітка: вона іноді перетворюється на SLEPT (соціальні, правові, економічні, політичні, технологічні), PESTEL (політичний, економічний, соціальний, технологічний, екологічний, правовий), STEEPLE (соціальний, технологічний, економічний,

екологічний, правовий, етичний) та ін.

9. Аналіз точки перегину. Точка перегину – це "подія, яка змінює спосіб, яким ми думаємо та діємо". Цей аналіз показує, коли і де, можливо, трапляться переломні моменти.

10. Гіперконкуренція. Використовуючи структуру конкурентних циклів Річарда д'Авена, аналітики можуть прогнозувати майбутню динаміку галузі [28].

Методи та інструменти конкурентної розвідки

Фахівці конкурентної розвідки зазвичай починають свою роботу зі збору інформації. Для досягнення цього необхідна мобілізація наявних джерел. Чим більше інформації збирається та аналізується фахівцями з питань розвідки, тим більше шансів отримати більш точну та детальну інформацію в інформаційному просторі. Часто великі корпорації використовують фахівців з різним досвідом роботи та різні методики роботи. Тут виникає небезпека отримання висновків на основі різних методологій, які зачастійше не базуються на будь-якій методології, а просто базуються на особистому досвіді окремих експертів. Зокрема, це видно в аналізі колишніх працівників спецслужб. Наприклад, методи аналізу даних, що використовуються спеціалістами конкурентної розвідки, які прийшли з поліцейських служб, зазвичай дуже відрізняються від методів колишніх працівників спецслужб. Це пов'язано з тим, що такі працівники мають дуже різний досвід, і використовувана методика також дуже відрізняється.

Часто важко довести представникам вищого керівництва необхідність використання спеціальних методів конкурентної розвідки та суб'єктів бізнесу, які, як правило, не знайомі з перевагами використання конкурентної розвідки, та очікують оцінити дії та стратегію конкурентів за допомогою традиційних засобів, але не отримують бажаного результату. Фахівці конкурентної розвідки вважають, що традиційні методи не можуть допомогти належним чином реагувати на несподівану агресивну тактику, яку використовує суперник. Це трапляється тому, що традиційні методи не оцінюють вплив зовнішніх факторів на успішну роботу підприємства. Такі фактори можуть бути різними: від особистих контактів до контактів на політичному рівні та подальших дій.

Спеціально освоєні методи аналізу конкурентної розвідки дозволяють правильно оцінювати зовнішнє середовище компанії чи корпорації, а отже,

допомагати приймати правильні стратегічні рішення. Для того, щоб використовувати методи аналізу конкурентної розвідки необхідно не тільки збирати й інтерпретувати показники та інформацію про фінансове становище підприємства, продажах і позиції на ринку, а й отримувати інформацію про дії конкурентів, дії моніторингових установ, технологій та інших факторів, які допомогають спеціалістам з конкурентної розвідки аналізувати та оцінювати зібрану інформацію, необхідну для аналізу належним чином.

Колишній поліцейський персонал часто використовує специфічну предметно-орієнтовану методологію, а колишній розвідувальний персонал часто використовує методологію, орієнтовану на процес.

Тому великі організації вимагають наявність спільної методології, яка б відповідала їхнім специфічним потребам, що допомагає спеціалістам з конкурентної розвідки збирати та аналізувати інформацію незалежно від того, який їх досвід і яка методологія застосовується.

Відкриті джерела інформації можуть бути одними з найважливіших джерел для спеціалістів конкурентної розвідки, які працюють у великих організаціях, тому що вони можуть збирати до 80% розвідувальної інформації, використовуючи лише відкриті джерела.

Таким чином, дуже важливо, щоб фахівці конкурентної розвідки аналізували загальнодоступну інформацію в першу чергу. За цією великою кількістю інформації про конкурентів, можна знати їх стратегії та заплановані дії [27].

Висновки до другого розділу

Встановлено, що успішне забезпечення ІБ сучасного підприємства є неможливим без здійснення цілеспрямованої, послідовної та кваліфікованої діяльності зі збору, обробки інформації з важливих питань життєдіяльності суб’єкта підприємництва та інформування керівництва з метою прийняття оптимальних управлінських рішень. У нинішніх умовах основний перелік завдань з інформаційно-аналітичного ЗІБ підприємства виконує конкурентна розвідка.

Конкурентна розвідка – є легальним процесом ідентифікації, збору, оцінки та поширення інформації про сильні та слабкі сторони конкурента, а також

інформацію про продукти та споживачів. Підприємства використовують конкурентну розвідку для того, щоб забезпечити надійний захист економічної та інформаційної безпеки і покращити свої позиції на ринку. Іншими словами, розвідка впливає на побудову власних планів і стратегій організації, що допомагає визначити можливі загрози, перш ніж вони стануть помітними та очевидними.

Процес конкурентної розвідки допомагає підприємству отримувати, обробляти, аналізувати, розповсюджувати та інтерпретувати інформацію конкурента, щоб реагувати відповідним чином.

Серед основних методів конкурентної розвідки варто відзначити: метод альтернативних ресурсів; метод аналізу можливості; контр-аналітичний метод; метод дивергенції; методи фактичного аналізу та аналізу конкурентних гіпотез; метод ідентифікації проблем тощо. Загалом у конкурентній розвідці використовують кілька десятків аналітичних методів.

Розділ 3
ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ КОНКУРЕНТНОЇ РОЗВІДКИ НА ПІДПРИЄМСТВІ

3.1 Процес впровадження конкурентної розвідки на підприємстві

Конкурентна розвідка є дуже важливою для ефективної діяльності підприємства. Це означає, що отримана за допомогою неї інформація повинна бути розширена в процесі, який називається аналіз розвідувальних даних [29], з визначною цінністю, яка перетворює ці дані на реальну розвідку – тобто прогнозування, яке є основою для стратегічних рішень верхівки управління компанії.

Загалом, до конкурентної розвідки пред'являються такі вимоги:

а) своєчасне визначення ключових проблем компанії, що виникають у бізнес-середовищі.

б) забезпечення можливих рішень цих проблем з точки зору розвідки.

Конкурентна розвідка – це методичний комплекс, призначений для комерційних цілей, який служить інструментом корпоративного управління при підготовці матеріалів, що сприяють прийняттю стратегічних рішень. Це може стосуватися інновацій, інвестицій, майбутнього напряму компанії, розвитку ринків, секторів, клієнтів, конкуренції, ділових партнерів тощо [30].

Конкурентна розвідка передбачає систематичне, творче та етичне застосування методології збору розвідданих та інших ключових методів, що використовує командну роботу для:

• збору й ідентифікування ознак, даних та/або джерел інформації;

• аналізу ознак, даних та зібраної інформацію, доповнення цих матеріалів, оцінювання їхньої значимості та їх організація як обгрунтування для деяких змін;

• формування гіпотез правдоподібних змін (перспективний стан) з наявної інформації та оцінки їх користі з точки зору супутніх фактів та витрат для встановлення ефективності цих змін;

• підготовка звітів про розвідку для підтримки процесу прийняття рішень щодо корпоративного управління.

У зв'язку з цим слід зазначити, що для особи, яка приймає рішення, інформація стає перевагою (зброєю) лише тоді, коли вона визнає її важливість як можливість отримати або створити конкурентоспроможну перевагу для бізнесу [31].

Впровадження конкурентної розвідки у бізнес-операції має свої підводні камені. Наприклад, важливим чинником є розмір компанії та ресурси, які вона може виділити для цього амбітного старту. Економічна потужність компанії, таким чином, перетворюється в більше варіантів впровадження або використання конкурентної розвідки як способу складання схеми майбутнього розвитку підприємства. Це досить складна справа, яка потребує збору даних та значну кількість інформації, проведення аналізу розвідки та проектування нових стратегій для суб'єктів підприємництва. Очевидно, для досягнення цих цілей перевагою буде робота в команді. Розроблена стратегія повинна бути як реалістичною, так і нездійсненною, тому команда повинна об'єднувати експертів з різних галузей, що переходять до даного виду бізнесу. Команду має очолити експерт – організована людина, яка знайома з робочим планом "Конкурентна розвідка", а також іншими заходами, що застосовуються в цьому виді робіт.

Роботу над пропозицією, як запровадити конкурентну розвідку в компанії, слід розпочати з уточнення одного основного питання: Хто буде одержувачем результатів цієї системи конкурентної розвідки? Відповідь на це питання визначатиме вид розвідки (стратегічна, оперативна), яку здійснюватиме команда з питань конкурентної розвідки.

Надалі треба з’ясувати, що насправді потрібно отримувачам звітів про розвідку. Це, по суті, питання про ключові теми розвідки. Чітко визначені

потреби в розвідці є стартовою точкою для професійної підготовки та впровадження всього процесу розвідки, або повного циклу конкурентної розвідки. Визначившись з інтелектуальними потребами вищого керівництва підприємства, можна почати пропонувати модель впровадження конкурентної розвідки у компанії [32].

Функція конкурентної розвідки може бути забезпечена:

1. Керівництвом компанії в обличчі команди (підходить для малого бізнесу), можливо, у співпраці з експертом із зовнішніх організацій.

2. Професійним підрозділом з питань конкурентоспроможності підприємства, створеним спеціально для цієї мети у співпраці як з персоналом компанії, так і із зовнішніми організаціями.

3. Зовнішньою організацією, що підписала контракт з компанією (наприклад, коледж, який виконує дослідницький проект тощо).

4. Призначеною командою співробітників компанії під експертним керівництвом фахівця з питань конкурентної розвідки від зовнішньої організації, або підготовленого співробітника компанії з питань конкурентної розвідки (координатора КР), або членами професійного підрозділу з питань конкурентної розвідки.

Залежно від обраного вище підходу до забезпечення функцій конкурентної розвідки необхідно визначити, як вони будуть реалізовуватися. Однак, перш ніж керівництво прийме рішення щодо форми впровадження КР, доцільно провести вступний семінар з обговоренням існуючого методу управління компанією, особливо стосовно критичних ситуацій, які передвіщають кожну зміну стратегії підприємства.

Керівництво має розуміти, що навіть будучи постійним постачальником для інших підприємств – це не обов'язково назавжди, і що повинен бути план на випадок втрати відносно комфортного контракту. Також має бути корпоративна директива, де вказано, як діяти у такій ситуації, яка не повинна містити нічого, що вважається таємним [33].

Форми впровадження конкурентної розвідки

У представленні всіх сучасних методів із категорії «дисципліни системного застосування» у корпоративну практику йде та ж сама закономірність. У цьому випадку можна використовувати досвід впровадження, наприклад, методичних комплексів, які регулюються певними стандартами.

Ці стандарти містять сукупність дій, які дозволяють компанії вести розробку, впровадження та підтримку систематичного процесу, що знаходиться в процесі безперервного виконання. Відповідальність за впровадження конкурентної розвідки має бути покладена на одну особу.

Програма впровадження КР в організації повинна містити:

• Інтеграцію та підготовку методичних процедур всередині організації та поза її межами.

• Встановлення цілей або показників, необхідних для оцінки результатів вжитих дій.

• Проекти чи дослідження, що проводяться у середовищі конкурентної розвідки.

• Порядок виконання запропонованих керівниками заходів щодо впровадження результатів проектів чи досліджень.

• Забезпечення механізму зворотного зв’язку щодо результатів розвідки.

• Визначення форм можливої співпраці із зовнішніми організаціями.

Реальний процес впровадження конкурентної розвідки поділяють на три фази: (Рис. 3.1.)

а) Управлінська підготовка до впровадження КР.

б) Особово-орієнтована та професійна підготовка до застосування КР.

в) Організаційна підготовка до впровадження та застосування КР.

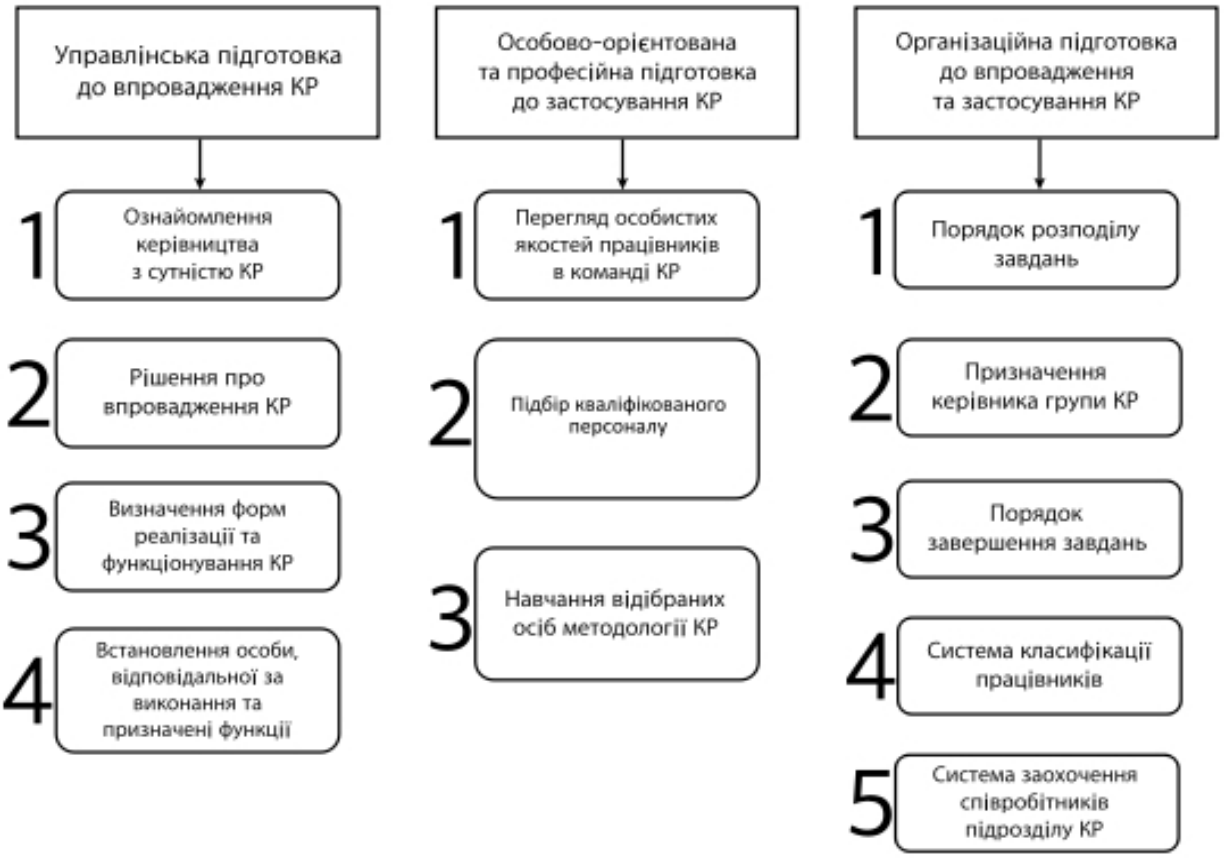

Рис. 3.1. Етапи процесу впровадження конкурентної розвідки на підприємстві

Управлінська підготовка до впровадження КР передбачає здійснення наступних кроків:

1. Ознайомлення керівництва компанії з сутністю КР.

2. Рішення про впровадження КР в компанії.

3. Визначення форм реалізації та функціонування КР.

4. Встановлення особи, відповідальної за виконання та призначені функції.

Особово-орієнтована та професійна підготовка до застосування конкурентної розвідки може включати наступні пункти:

1. Перегляд особистих якостей працівників для роботи в команді КР.

2. Підбір кваліфікованого персоналу для цієї роботи, всередині підприємства або за допомогою зовнішнього пошуку.

3. Навчання відібраних осіб методології КР та пов'язаних з нею заходів.

Організаційна підготовка до впровадження та застосування КР охоплює такі пункти:

1. Порядок розподілу завдань.

2. Призначення керівника групи КР.

3. Порядок завершення завдань.

4. Система класифікації працівників.

5. Система заохочення співробітників підрозділу КР [34].

Готуючись до реалізації конкурентної розвідки, слід почати з базового розуміння того, що безліч разів виявлялося істинним у діловій практиці – а саме те, що основою успішної інформаційної системи є корпоративна культура.

Це означає, що система базується, насамперед, на людях. Щоб система конкурентної розвідки була справді функціональною та корисною для підприємства, вона має бути заснована на трьох основних принципах: стабільності, довгострокової перспективи, причетності.

Працівники кожного бізнесу представляють безліч знань та цінної інформації про конкурентноспроможність. Завдання забезпечити і зафіксувати необхідні дані або інформаційні виклики для побудови широко розширеної корпоративної інформаційної мережі, щоб відповідні дані могли бути зібрані всередині компанії (зазвичай це завдання бізнес-розвідки). Створення так званої "розвідувальної карти компанії" допомагає досягти цілі цього завдання. У корпоративній практиці завдання вирішується за допомогою аудиту розвідки.

Проведення розвідки включає*:*

а) Класифікацію працівників за їхньою експертизою: технології, дизайн, економіка, торгівля, людські ресурси тощо.

б) Складання діаграм (карт) знань з кожної спеціальності, департаменту.

в) Визначення формального способу зберігання даних, інформації, знань.

г) Визначення диференційованого доступу до збереженої інформації для окремих користувачів.

Невід'ємна частина інтеграції конкурентої розвідки на підприємстві – це її захист, що охоплює юридичні, технічні та організаційні аспекти, а також персонал, безпеку та контррозвідку [35].

Найчастіші помилки, які роблять підприємства, коли впроваджують конкурентну розвідку.

При впровадженні системи конкурентної розвідки у практичному плані слід пам’ятати про деякі небезпеки та помилки, до яких схильні керівництво та працівники. Найбільш поширеними, іноді суперечливими, є такі:

1. Вищий та/або середній менеджмент підприємства не довіряє результатам КР.

2. Вищий менеджмент компанії має нереалістичне сприйняття, засноване на вірі, що підрозділ КР зручно вирішить усі проблеми компанії.

3. Співробітники КР докладають мінімальні зусилля для роботи з первинними джерелами даних.

4. Більшість часу працівники КР витрачають на виконання оперативних завдань, а не на підготовку матеріалів для стратегічних рішень вищого керівництва компанії.

5. Нездатність максимально використати всі переваги та можливості, які пропонує КР (використання всього її розвідувального потенціалу).

6. У багатьох випадках наведена потужність КР (підсумковий звіт, якщо він готовий) є продуктом синтезу, а не аналізу. Це означає, що результат, отриманий за допомогою розвідувального аналізу, має бути створеним (як правило, внаслідок досить складного процесу), а не лише продуктом, скомпільованим з частин зібраних даних.

7. Підсумковий звіт не стосується можливих майбутніх кроків конкуренції (у гіпотетичній формі) та оцінки її потенційного впливу на розвиток бізнесу, оскільки він стосується бізнес-секторів, конкурентів, постачальників, замовників та бізнесу загалом. У звіті також мають бути запропоновані можливі відповіді на кроки конкурентів.

8. Передчасна і зазвичай недоцільна покупка дорогого програмного забезпечення для конкурентної розвідки.

9. Некритичне прийняття сучасних «західних» методів без достатніх знань та/або впевненості у застосуванні.

10. Вищому менеджменту не вдається створити сприятливих умов для успішного введення в дію діяльності КР (освіта, навчання, забезпечення обладнанням, інструментами, ресурсами тощо).

3.2 Корпоративна контррозвідка як інструмент запобігання та протидії методам недобросовісної конкуренції

Як зазначалося, однією зі складових конкурентної розвідки на підприємстві є контррозвідка, яка в межах бізнес-підрозділів може бути визначена як виявлення та нейтралізація численних загроз, які створюють спецслужби будь-яких конкурентів, та маніпулювання цими службами на користь маніпулятора [36].

Автори стверджують, що корпоративна контррозвідка є іншою стороною конкурентної розвідки, оскільки вона представляє процес, завдяки якому компанії захищають свою внутрішню інформацію [37].

Корпоративна контррозвідка має як активні, так і пасивні характеристики. Експерти з корпоративної безпеки одноголосно стверджують, що пасивна контррозвідка впроваджує оборонні тактики та інструменти, такі як програмні рішення, контрспостереження та тестування на можливість проникнення. Активна контррозвідка, навпаки, здійснює наступальну тактику та надалі розслідує будь-які протиправні, неетичні чи загрозливі дії щодо її джерел [36].

Класичний процес контррозвідки на всіх рівнях включає чотири етапи:

1) оцінка контррозвідувального захисту;

2) проведення контррозвідувальних спостережень;

3) розробка плану контррозвідки;

4) здійснення відповідних контррозвідувальних заходів [38] (Рис.3.2.).

Деякі спеціалісти з конкурентної розвідки пропонують використовувати цикл контррозвідки спільно з класичним циклом конкурентної розвідки.

Іншими словами, найголовніша мета підрозділу контррозвідки – забезпечити активну протидію загрозам та загальне посилення безпеки підприємства, захищаючи активи не лише від злочинів, але й від цілком законних зусиль конкурентної розвідки бізнес-конкурентів.

За логікою, корпоративна контррозвідка разом з конкурентною розвідкою має бути інтегрована в стратегію організацій. Ставлення будь-якого іншого підприємства до цього питання може бути руйнівним для її подальшого існування.

Рис. 3.2. Класичний процес контррозвідки

Незалежно від того, чи заподіяло економічне, промислове чи корпоративне шпигунство шкоду корпоративним інтересам, підприємство має протидіяти таким спробам. Конкурентну розвідку та контррозвідку слід впроваджувати в рамках стратегії ІБ компаній, але її не слід плутати із ІБ в цілому. Незалежно від того, чи стратегія є оборонною чи наступальною, обидва інструменти можуть мати пасивні чи активні компоненти. (Рис. 3.3.)

Рис 3.3. Активні й пасивні компоненти контррозвідки

Активні компоненти зосереджуються в основному на активних та проактивних заходах, які включають:

• Корпоративні розслідування – дають інформацію про найцінніші активи компаній - їх людський ресурс. Це дуже корисний проактивний інструмент, який зменшує ризики, пов'язані з працівниками, за допомогою біографічних фактів, попередніх перевірок та ретельних досліджень, перш ніж працевлаштовувати працівника.

• Конкурентні розвідувальні та контррозвідувальні операції повинні впроваджувати ефективну політику та процедури класифікації інформації. Такі заходи можуть реалізувати нову корпоративну культуру, пов’язану з активним захистом інформації працівниками.

• Колективний етичний процес може бути впроваджений, коли відповідальний підрозділ безпеки знайде докази незаконного збору конфіденційної інформації. Тобто, співробітники з контррозвідки мають

повідомити правоохоронні структури, які в подальшому можуть застосувати власні контрзаходи.

Пасивні компоненти зосереджуються переважно на профілактичних заходах. Ці заходи можуть включати в себе:

• Ситуаційна обізнаність персоналу щодо загроз шпигунства. Усі заходи та практики безпеки стають марними без належним чином навченого персоналу. Такі тренінги слід проводити регулярно, щоб покращити знання працівників як про тактики конкурентної розвідки, так і про незаконні методи збору інформації.

• Захисні заходи включають низку програм, які визначають можливі загрози серед персоналу та пов'язані з цим ризики, що можуть бути сприйнятливими для зовнішнього впливу.

• Технічні контрспостереження складаються з комплексу заходів щодо виявлення незаконних технічних пристроїв, встановлених для збору інформації. Мета технічного контрспостереження – запобігти будь-яким технічним втручанням, які представляють собою останній можливий інструмент промислових шпигунів, коли їх зв'язок до цільовою організацією припиняється.

• Тестування на проникнення застосовується для оцінки вразливих ситуацій, що є критичними для конкурентних переваг, галузей та заходів. Більшість систем безпеки не можуть протидіяти професійній команді шпигунів. Однак регулярне тестування на проникнення може оцінити поточну ефективність системи безпеки та покращити практику контррозвідки щодо потенційних суб’єктів промислового шпигунства [36].

Зрештою, як зазначають деякі автори, готовий продукт розвідки є найважливішим інструментом прийняття рішень. Завершена та оброблена розвідка розбита на п’ять загальних категорій:

1) Поточна розвідка – надання менеджерам різних рівнів інформації про виникаючі зміни, які можуть мати вплив на корпоративну стратегію, тактику чи операції;

2) Оцінювальна розвідка – комплексний аналіз та довгострокове прогнозування, розроблене для вищого менеджменту, для допомоги їм у подальшому прогнозуванні можливих перспектив та загроз;

3) Дослідницька розвідка – класифіковані дослідження, які поділяються на два підтипи: базово-дослідницька розвідка та оперативно-розвідувальна розвідка;

4) Науково-технічна розвідка – вирішальна для інноваційних компаній, що працюють у науковій чи технологічній галузях; пов'язані з дослідженнями та розробками конкурентів;

5) Попереджувальна розвідка – включає контрольний список попереджень та попередження про небезпеку загалом.

Контррозвідка має на меті запобігання та протидію випадкам недобросовісної конкуренції на підприємстві.

Недобросовісна конкуренція – це будь-яка шахрайська, оманлива чи нечесна практика, заборонену статутом, положенням чи загальним законодавством. Вона складається з суміжних доктрин, що породжує декілька різних причин дій, включаючи дії з порушення патентів, товарних знаків або авторських прав; дії з неправомірного присвоєння торгових найменувань, торговельних та комерційних таємниць та дії щодо публікації наклепницьких, помилкових чи оманливих заяв [39].

Основні види бізнес-порушень, які є прикладами «недобросовісної конкуренції».

1. Порушення торгової марки

Викрадання конкурентом об’єкта інтелектуальної власності іншої компанії і використання його для отримання прибутку чи покращення позицій на ринку. Прикладом цього є використання конкурентом чужого логотипа або слогана у власних ресурсах, медіа тощо.

2. Недобросовісна реклама

Ствердження та використання конкурентом нечесної чи неправдивої інформації щодо його продукції чи послуг.

3. Несанкціонована підміна

Іноді цей вид називають «заманити та підмінити», оскільки цей незаконний метод передбачає, що конкурент навмисно вводить в оману потенційних клієнтів та представляє свій «якісний» продукт, а після продажу – підміняє товар на товар з меншою якістю. Ця тактика часто поєднується з порушенням торговельної марки.

4. Неправомірне присвоєння комерційної таємниці

Отримання та використання конкурентом внутрішніх знань компанії, включаючи формули, засоби, стратегії тощо, захищені законодавством про інтелектуальну власність, задля власної вигоди та грошового прибутку.

5. Надання неправдивої інформації

Випередження конкурента на ринку шляхом подання неправдивих відомостей або надання недоброякісних гарантій якості. Цей тип недобросовісної конкуренції часто включає: гарантії продукту, гарантії якості та інші засоби комерційної політики [40].

Зневага конкурента, присвоєння комерційної таємниці та порушення торговельної марки – все це підпадає під недобросовісну конкуренцію, що створює неправильне враження у споживачів про конкурента та його продукцію. У 2009 році компанія PepsiCo подала до суду на Coca-Cola за те, що вони рекламували свій спортивний напій Powerade як більш освіжаючий, ніж Gatorade виробництва PepsiCo через наявність у напої виробництва Coca-Cola більшої кількості електролітів. Експерти PepsiCo стверджували, що за цим твердженням немає жодних наукових доказів [41].

3.3 Кращі практики надання послуг конкурентної розвідки на аутсорсинговій основі

Великі підприємства і корпорації часто віддають перевагу залученню для виконання функцій конкурентої розвідки консалтингових фірм і спеціалізованих компаній на аутсорсинговій основі. У результаті тендерів на

здійснення завдань зі збору й аналізу конкурентної інформації компанія-замовник обирає найбільш прийнятний для себе варіант.

Особливу роль на ринку послуг конкурентної розвідки відіграють компанії, які, крім надання основних послуг, також можуть запропонувати свої авторські і додатково розроблені спеціальні програми.

Серед компаній-професіоналів, які надають найбільш якісні та часто ексклюзивні сервіси в цій галузі, варто виділити такі:

1. Aurora WDC

Особливості компанії: три пропозиції Aurora WDC (AuroraGPS, FirstLight та RECONVERGE) були спеціально розроблені для задоволення потреб фахівців з розвідки та вищих посадових осіб.

Девіз: Aurora WDC готова допомогти вам прорватися.

Основні послуги: збір та аналіз конкурентної розвідки, платформа FirstLight SaaS, спільнота соціального навчання RECONVERGE.

Місія: Обслуговувати організації по всьому світу, вигравати у ринковому середовищі, застосовувати технології для розширення результатів та побудови культури розвідки.

2. Tyson Heinz

Особливості компанії: їх спадщина в конкурентній галузі оцінюється чотирма десятиліттями, починаючи від ролі ініціатора галузі до нових практик сьогодення.

Основні послуги: аналіз/профілювання конкурентів, дослідження ринку, порівняльний аналіз конкурентів.

3. MindShifts

Особливості компанії: MindShifts – це австралійська провідна консалтингова фірма з питань конкурентної і стратегічної розвідки та всесвітньо визнаний гравець у сфері керівного коучингу.

Їх клієнти: CAT, Ernst & Young, Johnson & Johnson, 3M, Novartis.

Основні послуги: Коучинг, семінари з стратегічного планування, наставництво в КР, військові ігри, доповіді з ключових питань, семінари з КР.

4. M-Brain

Особливості компанії: M-Brain – це глобальна компанія з інформаційних послуг, що має офіси в 15 країнах і надає послуги, засновані на унікальному поєднанні власних технологій обробки великих даних та агентурною розвідкою.

Їх клієнти: IBM, Nestle, Hitachi, Pfizer, Philips, Samsung, American Express, Bosch.

Основні послуги: дослідження ринку, медійна аналітика.

5. Intelligentsia

Особливості компанії: Intelligentsia надає клієнтам вагомі результати та поради, завдяки яким можна отримати ефективний розвиток свого бізнесу, перевагу над конкурентами та зниження ризиків ключових рішень.

Ключові галузі: споживча та роздрібна торгівля, енергетика, фінансові та професійні послуги, охорона здоров'я, технології та засоби масової інформації

Основні послуги: Конкурентна розвідка, аналіз конкурентів, дослідження ринку, попередня комерційна оцінка.

6. I-Intelligence

Особливості компанії: I-Intelligence присвятила себе допомагати клієнтам вдосконалити свої можливості збирати, аналізувати, керувати, обмінюватися та передавати інформацію, будь то в підтримку урядової політики чи заради конкурентних переваг.

Ключові галузі: державні установи, міжнародні організації, приватні організації.

Основні послуги: Конкурентна розвідка, моніторинг конкурентів, моніторинг соціальних медіа.

7. Helicon Group

Особливості компанії: Helicon Group надає знання про КР та опублікувала кілька книг про конкурентну розвідку.

Основні послуги: навчання та консалтинг, професійне наставництво.

Девіз: Конкурентна розвідка для конкурентних переваг.

8. Fuld & Co

Особливості компанії: Fuld & Company допомагає клієнтам орієнтуватися у порушеннях та створювати надійні та конкретні стратегії, щоб в подальшому конкурувати в їх динамічному ринковому середовищі.

Основні послуги: аналітична картина ринку, конкурентна розвідка, стратегічне планування.

Ключові галузі: медичні послуги, енергетика, фінансові послуги, споживчі товари.

9. European Agency

Особливості компанії: EASI – це команда експертів з веб-стратегій, яка підтримує та допомагає клієнтам усвідомити причетність мережі до загальної стратегії компанії.

Їх клієнти: LG, GlaxoSmithKline, Grand Marnier, Banque de France.

Основні послуги: комунікація, стратегічна розвідка, інструменти взаємодії, навчання.

10. Aqute Intelligence

Особливості компанії: Aqute Intelligence робить дійсно детальний, характерний вид конкурентної розвідки, використовуючи достовірні та рідкі факти.

Їх клієнти: Intel, BBC, Ford, Coca-Cola, Microsoft, Johnson & Johnson, IBM.

Ключові галузі: технології, фінансові послуги, роздрібна торгівля, виробництво, фармацевтика [47].

Висновки до третього розділу

З’ясовано, що процес реалізації конкурентної розвідки на підприємстві складається з трьох етапів, якими є: підготовка керівника до впровадження конкурентної розвідки; особово-орієнтована та професійна підготовка до застосування конкурентної розвідки; організаційна підготовка до впровадження та застосування конкурентної розвідки.

Управлінська підготовка до впровадження КР передбачає ознайомлення керівництва компанії з сутністю КР; прийняття рішення про впровадження КР в компанії; визначення форм реалізації та функціонування КР; встановлення відповідальних осіб / особи. Особово-орієнтована та професійна підготовка до застосування конкурентної розвідки може включати оцінку бажаних особистих якостей працівників для роботи в команді КР, підбір і, за потреби, навчання персоналу. У рамках організаційної підготовка до впровадження та застосування КР встановлюють порядок розподілу і завершення завдань; призначають керівника групи КР; розробляють систему класифікації і заохочення співробітників підрозділу КР.

Однією зі складових конкурентної розвідки на підприємстві є контррозвідка, яка має на меті виявлення та нейтралізацію численних загроз, які створюють спецслужби будь-яких конкурентів, та маніпулювання цими службами на користь маніпулятора.

Класичний процес контррозвідки на всіх рівнях включає чотири етапи, серед яких: оцінка контррозвідувального захисту; проведення контррозвідувальних спостережень; розробка плану контррозвідки; здійснення відповідних контррозвідувальних заходів. Основним видом загроз, яким має запобігати та протидіяти корпоративна конттрозвідка є недобросовісна конкуренція, до якої відносять будь-яку шахрайську, оманливу чи нечесну практику, заборонену статутом, положенням чи загальним законодавством (неправомірне присвоєння комерційної тамниці, надання неправдивої інформації тощо).

З моменту формування конкурентної розвідки на професійній основі на ринку з'являються компанії, які займаються КР на аутсорсинговій основі і консалтингові фірми. Кращі з них обслуговують підприємства і різних клієнтів по всій земній кулі, навчають керівників різних корпорацій орієнтуватися на ринку і в конкурентному середовищі, а також допомагають їм у формуванні успішного стратегічного планування у конкурентній розвідці.

Розділ 4
ПРИКЛАДНІ ІНСТРУМЕНТИ КОНКУРЕНТНОЇ РОЗВІДКИ

4.1 Засоби пошуку й обробки розвідувальної інформації в мережі Інтернет

Пошук інформації в мережі Інтернет без використання пошукових ресурсів, тільки шляхом перегляду окремих веб-сайтів, по-перше, носить вибірковий і/або випадковий характер (до того ж інформація на окремих сайтах може мати досить суб'єктивний або навіть замовний характер), по-друге, вкрай не продуктивний – навряд чи можна обійти і повністю переглянути більше сотні веб-сайтів за день безперервної роботи, навіть якщо знати їх адреси.

Усі існуючі ресурси пошуку інформації в Інтернеті можуть бути умовно розділені на кілька підгруп, а саме:

- ресурси пошуку інформації на окремих сайтах;
- добірки посилань;
- каталоги;
- пошукові системи;
- мета-пошукові системи;
- системи моніторингу та контент-аналізу;
- екстрактори об'єктів, подій і фактів;
- системи Knowledge Discovery, Data Mining, Text Mining;
- спеціалізовані системи конкурентної розвідки;
- інтегровані системи [24].

На перших етапах розвитку конкурентної розвідки та інформаційної революції загалом фахівці з КР мали в своєму арсеналі найпростіші і малофункціональні способи пошуку інформації: на окремих сайтах, використовуючи підбірки посилань та каталоги. Дані методи використовувалися регулярно і на їх зміну на постійній основі прийшли

пошукові та метапошукові системи, але для детальної ручної перевірки даних розвідки їх місце в існуванні залишилося [42].

За своєю суттю каталоги, пошукові системи і мета-пошукові системи є веб-сайтами зі спеціалізованими базами даних, в яких зберігається інформація про інші веб-ресурси і документи, що зберігаються на них. В результаті запиту до таких систем видається список адрес, а іноді і короткий опис документів (сніппети), де може бути присутньою запитувана інформація. Як правило, пошук може проводитися тільки за ключовими словами і фразами. Активізуючи на посилання, знайдену в результаті запиту, користувач потрапляє на оригінал документа, розміщеного на деякому веб-сайті. Звісно, якщо документ згодом змінився або веб-сайт припинив своє існування, то заіндексований пошуковою системою документ через деякий час може бути не знайдений.

Основна відмінність пошукових систем від каталогів – наявність автоматичного «робота», постійно скануючого веб-простір і накопичуючого нову інформацію в індексних файлах бази даних. В каталоги ж інформація заноситься вручну, чи власниками сайтів, або обслуговуючим персоналом самих каталогів. Користування такими системами, як правило, безкоштовне, це найпопулярніші пошукові інструменти в мережі Інтернет.

Метапошукові системи є пошуковими системами по пошуковим системам. Так як окремі пошукові системи по-різному індексують хоча і великі і часто пересічні, але все-таки різні сегменти мережі, то, звісно, і результат пошуку за допомогою метапошукової системи буде, апріорі, повнішим, ніж за допомогою однієї окремо взятої пошуковиї системи. Враховувати це плюсом чи мінусом пошукової роботи залежить від поставлених цілей і кількості знайдених документів. Якщо в результаті пошуку знайдені тисячі або мільйони документів, то «вручну» все одно навряд чи можна переглянути понад декілька сотень.

Іншою пошуковою перевагою таких систем є те, що одним запитом забезпечується пошук у багатьох пошукових системах, не вимагаючи численних повторень одного і того ж запиту в різних пошукових системах.

Пізніше у використанні з'явилися системи моніторингу та контент-аналізу. Продукти-ПЗ, що здійснюють пошук інформації як сервіс, використовуючи дані методи – знаходяться на хороших позиціях на ринку, враховуючи навіть те, що їх функціональність і складність не є такою передовою, порівняно з іншими методами сьогодення.

Системи моніторингу та контент-аналізу забезпечують регулярний пошук і «скачування» інформації по заданим темам і з заданих сайтів, а також аналіз змісту «скачуваних» документів. Такі системи, як правило, володіють розвиненою мовою запитів, що дозволяє істотно деталізувати і конкретизувати запити в порівнянні зі звичайними пошуковими системами. По-друге, такі системи зберігають у своїх базах даних повні тексти початкових документів, що забезпечує збереження цих документів у часі і можливість їх обробки і контент-аналізу, як в поточному часу, так і в ретроспективі. Істотною перевагою таких систем є також те, що склідні запити, що складаються з десятків або сотень пошукових слів та виразів, одного разу складені знавцем-аналітиком предметної галузі, можуть бути збережені у вигляді каталогізованого запиту або рубрики й надалі визиватися автоматично або вручну зі збереженого списку для проведення пошуку або контент-аналізу.

За допомогою контент-аналізу такі системи дозволяють встановити пересічні зв'язки між темами, поняттями і об'єктами, поставленими на моніторинг, виявляти емоційне забарвлення документів, проводити аналіз динаміки появи в часі тих чи інших документів, проводити порівняльний аналіз інформаційної активності по різних тематик і багато іншого.

Якщо моніторингові системи як системи фільтрації можуть виділяти з інформаційного потоку відомі об'єкти, то екстрактори об'єктів, подій і фактів вміють виділяти з потоку інформації об'єкти, невідомі заздалегідь, події або

факти, які відповідають лише певному заздалегідь типу, наприклад, географічні поняття, персони, структури і організації, події (дорожньо-транспортні події, катастрофи, міжнародні зустрічі). При цьому факти можуть класифікуватися як звичайні або незвичайні. Прикладом простого факту у даному випадку можна вважати виїзд автомобілів за межі міста, а прикладом незвичайного факту – виїзд за ту ж межу міста автомобіля без номерних знаків [24].

На цей час активно використовуються системи, які займаються виявленням та аналізом даних: Knowledge Discovery, Data Mining, Text Mining. Так само, як і використаня спецальних новітніх засобів у вигяді додатків, програмного забезпечення та інших спеціалізованих систем. Найпоширенішим методом збору інформації є використання пошукових систем, найбільш відомими прикладами яких є Google і Yahoo!. Ці пошукові системи приймають запит користувача, ключові слова і відповідають набором веб-сторінок або документів, які певною мірою задовольняють запит. Далі цей набір сторінок і документів певним чином організований.

Системи типу Knowledge Discovery, технології Data Mining і Text Mining, вміють виявляти нові знання і закономірності. Така система, наприклад, може самостійно, без участі людини, зробити висновок про факт знайомства між людьми, грунтуючись на наявних в системі даних про закінчення ними однієї і тієї ж школи, одного класу в одному і тому ж населеному пункті. Правда, самі правила, за якими така система робить висновки, все-таки створюються і задаються поки що людьми.

Спеціалізовані системи для конкурентної розвідки можуть включати в себе один або декілька з перерахованих вище пошукових засобів, спеціально «заточених» під ці специфічні завдання. Крім того, потреби конкурентної розвідки припускають використання в якості джерел інформації, крім повнотекстових документів, ще й доступних в мережі Інтернет баз даних (БД), власних, що належать компанії, документів, таблиць і баз даних, а

також формалізованих і неформалізованих документів і БД, здобутих з інших джерел. [24]

Пошукова системи зазвичай складається з наступних компонентів.

1. Пошукові модулі або пошукові роботи, які використовуються для збору веб-сторінок за допомогою методів пошуку графів.

2. Метод індексації, який використовується для індексації зібраних веб-сторінок та зберігання індексів у базі даних.

3. Методи пошуку та ранжування, які використовуються для отримання результатів пошуку з бази даних та представлення рейтингових результатів користувачам.

4. Інтерфейс користувача, який дозволяє користувачам здійснювати пошуковий запит у базі даних та налаштовувати їх пошук [42].

Окрім загальних типів пошукових систем, доступний ряд доменних систем. Прикладами цього є:

• Northern Light – пошукова система для комерційних видань у сферах бізнесу та загального інтересу.

• EDGAR – це кліринговий центр комісії з цінних паперів та бірж Сполучених Штатів із загальнодоступною інформацією про компанії та їх поданих заявок.

• Westlaw – пошукова система серед юридичних матеріалів.

• OVID Technologies дає можливість об'єднувати пошук у багатьох субполів та базах даних медичної інформації.

Третій тип пошукової системи – це метапошукова система. Два приклади: MetaCrawler та Dogpile. Коли метапошукова система приймає запит, вона підключається до декількох популярних пошукових систем і інтегрує результати, отримані цими пошуковими системами. Метапошукові системи не зберігають власні індекси, але фактично використовують індекси, створені пошуковими системами, які використовувались для відповіді на запит.

Зважаючи на велику кількість сторінок, які може генерувати неконтрольований пошук, його слід необхідно контролювати. Це можна

здійснити за допомогою техніки контролю пошуку графів. Контроль пошуку – це фактично елементарний аналіз отриманої інформації. Фактично, пошук повинен відповідати лише тими сторінками, які мають відношення до запиту. Розумні пошукові системи здатні певною мірою працювати таким чином. Ця початкова форма аналізу називається веб-майнінг [43].

Веб-майнінг – це аналіз веб-ресурсів. Веб-майнінг можна класифікувати на три класи: аналіз контенту, аналіз структур та аналіз статистики відвідування. (Рис. 4.1.)

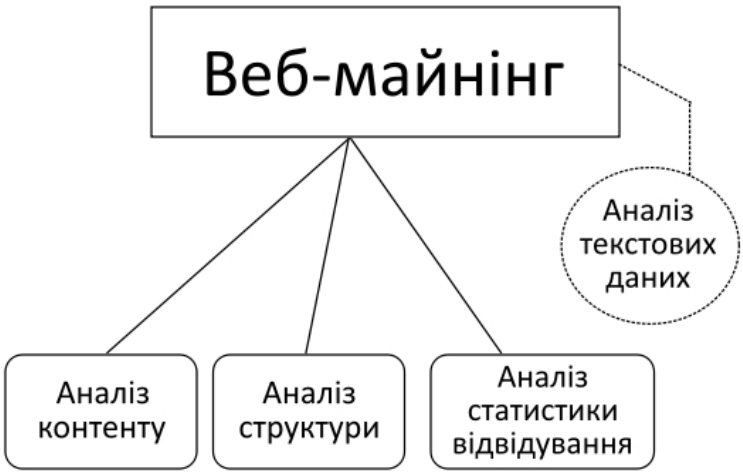

Рис 4.1. Класифікація веб-майнінга

1. Аналіз контенту

Аналіз контенту вдосконалює основну техніку пошуку. Також, аналіз контенту може поділятися на аналіз контенту веб-сторінок та на аналіз результатів пошуку. Аналіз наповнення веб-сторінки може розглядатися як аналіз самого тексту. Аналіз контенту веб-сторінок алгоритм пошуку графіків керується змістом сторінки. Непрофілізована пошукова система використовуватиме ключові слова для керування алгоритмом пошуку графів. Ця методика відповідає набором сторінок, які можна або шукати знову за допомогою уточнення початкового пошуку, або цей набір отриманих сторінок можна проаналізувати використовуючи складніші методи аналіз тексту.

2. Аналіз структури

Аналіз структури використовує логічну мережеву модель для визначення важливості веб-сторінок. Одним із методів є метод PageRank [44]. Ця методика визначає важливість мережевої інформації на основі кількості

посилань, які вказують на цю сторінку. Ідея полягає в тому, що чим більше сторінок, на які посилається дана веб-сторінка, тим більша її важливість. Ця методика в поєднанні з пошуком ключових слів є основою пошукової системи Google [45].

3. Аналіз статистики відвідування

Аналіз статистики відвідування сайтів виконує пошук даних у веб-журналах. Веб-журнал містить дані з відомостями про відвідування сайтів. Відомості про відвідування сайтів – це послідовність посилань сторінки, пов’язаних або з сервером мережі, або з клієнтом мережі (браузер). Ці дані можуть бути проаналізовані, щоб забезпечити інформацію про сервера або клієнта мережі залежно від того, які сторінки були відвідані.

Аналіз текстових даних

В деяких випадках навіть самий ретельно розроблений запит, надісланий добре сконструйованій пошуковій системі, приводить до сотні, якщо не тисячі результатам пошукових відповідей.

Метою аналізу текстових даних є проведення автоматизованого дослідження природно-мовних текстів. Цей аналіз призводить до зведення документів, що визначає, в якій мірі документ відповідає запиту користувача, а також відбувається кластеризація документів.

Незалежно від того, наскільки оптимально та/або ефективно виконується завдання інфомаційного аналізу, його корисність визначається якістю отриманої інформації. Через непідконтрольну розробку веб-сайтів та простоту посилань на інші сторінки користувач не має простого способу визначити, чи інформація, що міститься на веб-сторінці, є точною. Можливі неточності можуть бути випадковими або навмисними. Неточності є суттєвою проблемою, коли Інтернет використовується як джерело інформації для проекта конкурентної розвідки. І врешті-решт, проблема аналізу текстових даних – це перевірка інформації.

4.2 Програмні інструменти конкурентної розвідки для розширених досліджень ринку

За підсумками 2019 року на ринку наявна величезна кількість інструментів для конкурентної розвідки. Це може бути спеціалізоване програмне

забезпечення чи просто додатки.

З них можна виділити найпопулярніші і кращі у використанні:

1. Hootsuite – розвідка соціальних мереж.

Hootsuite – популярний безкоштовний веб-інструмент конкурентної розвідки та програмне забезпечення з пошуку інформації в соціальних мережах, яке агрегує контент з усього світу.

Цей інструмент дозволяє збирати цінну інформацію про те, що говорять конкуренти і клієнти у соціальних мережах в режимі реального часу.

Hootsuite – один з найкращих інструментів стеження за соціальними медіа, який охоплює багато соціальних мереж, таких як Twitter, Facebook, LinkedIn, WordPress, Foursquare та інших.

2. Google Alerts

Google Alerts – це одна з найпопулярніших безкоштовних служб оповіщення, яка дозволяє стежити за згадками в Інтернеті практично про все, що завгодно: компанію, бренд, клієнтів, конкурентів, закупівлі тощо.

Прикладом інших подібних сервісів до Google Alerts є Mention та Talkwalker Alerts. Вони надають навіть розширені функції для відстеження згадок в онлайн-середовищі.

3. Fanpage Karma – розвідка соціальних медіа.

Fanpage Karma – це інструмент розвідки у соціальних медіа. Завдяки Fanpage Karma можна не тільки проаналізувати свої профілі та профілі конкурентів, але і керувати усіма комунікаціями клієнтів за допомогою одного інструменту.

Fanpage Karma може проаналізувати конкурентів у Facebook, Google+, Twitter, Instagram, YouTube і навіть Pinterest.

4. Mediatoolkit – згадки про конкурентів.

Mediatoolkit – це потужний інструмент конкурентної розвідки для моніторингу онлайн-згадок про конкурента в режимі реального часу. Mediatoolkit гарантує знання про кожну статтю, хештег та коментар, що стосуються імені, яке відстежується.

Завдяки Mediatoolkit можна знайти згадки з будь-якого джерела світу: профілі у Facebook, Twitter чи Instagram, або оновлення веб-сайтів, блогів та форумів.

За допомогою Mediatoolkit також є можливість порівнювати себе з конкурентами, відстежувати актуальні теми галузі, знаходити цікаві пости та агентів впливу (інфлюєнсерів) в соціальних мережах у соціальних мережах і аналізувати структуру поведінки підприємств.

5. Crayon Intel Free – моніторинг контенту і змін дизайну конкурентів.

Crayon – це платформа розширеного дослідження ринку, яка допомагає підприємствам відстежувати та аналізувати діяльність конкурента. Crayon Intel Free дозволяє отримати конкурентну розвідку, включаючи публікації в блогах та відеоконтент. Також є можливість отримувати щоденні дайджести на електронну пошту.

Більше того, цей програмний інструмент дозволяє зібрати колекцію найжорсткіших конкурентів чи улюблених брендів. Можна відстежувати будь-яку кількість компаній.

Також, є версія Crayon Intel Pro, що є одним із найбільших інструментів дослідження ринку та конкурентної розвідки з потужним аналізом.

6. Visualping – відстеження змін сайту конкурента.

Visualping дозволяє відстежувати зміни на сайті конкурента. Visualping – це новий, простий у користуванні та дуже зручний інструмент для моніторингу змін на веб-сайтах.

Їх додаток у Chrome дозволяє відстежувати сторінки лише в один клік безпосередньо зі сторінки, яку треба відстежувати. Користувачі отримують лист на електронну пошту, коли виникають якісь зміни.

Цей додаток відрізняє від інших той факт, що він виявляє візуальні, а не текстові зміни.

7. Feedly – моніторинг контенту конкурента.

Feedly – це чудовий інструмент, який дозволяє бути в курсі всіх важливих тем, включаючи контент конкурента.

Можна дуже легко стежити за новинами про свою компанію або своїх конкурентів. Також, є можливість використовувати Feedly для пошуку нових конкурентів.

8. SimilarWeb.com – відстеження трафіку конкурентів.

SimilarWeb.com – це один із найкращих інструментів розвідки, коли мова йде про моніторинг трафіку веб-сайтів конкурентів.

За допомогою цього інструменту можна: орієнтуватися на конкурентів та галузь; розкривати аналітику та онлайн-стратегію конкурентів; відкривати для себе нових партнерів; виявляти тенденції; зрозуміти споживчі наміри та інше.

SimilarWeb – це дуже просте у використанні програмне рішення. Воно отримує статистику будь-якого веб-сайту за допомогою лише одного натискання.

9. Додаток про конкурентну розвідку SEMrush забезпечує уявлення про трафік конкурентів. Пакет SEMrush CI включає два інструменти.

SEMrush Traffic Analytics звітує про статистику трафіку веб-сайту та цифрові показники ефективності будь-якого домену та допомагає отримати ширший огляд конкурентів або потенційних партнерів.

SEMrush Market Explorer перераховує всіх відповідних виробників та їх ринкові характеристики, створює портрет аудиторії на ринку. Цей інструмент краще використовувати при дослідженні нового ринку.

10. SiteAlerts - відстеження трафіку конкурентів.

Інструмент конкурентної розвідки SiteAlerts дає миттєву інформацію про будь-який веб-сайт. Він дає відповіді на такі питання як "Скільки трафіку вони отримують?", "Звідки він береться?", "Які інструменти вони використовують?" та багато інших.

Можна легко відстежувати статистику, джерела трафіку, статистику соціальних медіа, згадки тощо.

SiteAlerts також дозволяє бачити, які технології використовують конкуренти.

11. Дослідницький центр Pew – відстеження основних тенденцій ринку.

Дослідницький центр Pew – це потужний інструмент, який можна використовувати для відстеження основних тенденцій ринку. Він надає інформацію про проблеми, погляди та тенденції, що формують світ.

Вони проводять аналіз контенту, демографічні дослідження та інші соціально-наукові дослідження, орієнтовані на дані.

12. SurveyMonkey – потужний інструмент онлайн-опитування.

SurveyMonkey – популярний інструмент, який чудово підходить для конкурентної розвідки і дозволяє проводити будь-який тип Інтернет-опитування з метою дослідження ринку, конкурентного аналізу чи оцінки відгуків клієнтів.

Платформа дуже проста у використанні, і величезний обсяг зібраних даних можна легко проаналізувати за допомогою сучасних методів аналізу даних.

13. Qualtrics Research Core – одна з найкращих платформ дослідження ринку підприємств.

Qualtrics Research Core – одна з найбільш надійних та найкращих платформ дослідження ринку підприємств по всьому світу. Цей інструмент дозволяє отримати дані, необхідні для прийняття ключових бізнес-рішень.

Qualtrics має все необхідне для всебічної конкурентної розвідки в Інтернеті: від тестування продуктів до зворотного зв’язку з клієнтами та відстеження торгової марки конкурента.

Платформа також використовує штучний інтелект для аналізу даних опитувань, щоб прогнозувати тенденції на ринку.

Ціна: основні безкоштовні опціони та преміальні плани.

14. Glassdoor – один з найбільших та найпопулярніших у світі сайтів для пошуку роботи та підбору персоналу. Він надає безкоштовну базу даних з мільйонами оглядів компаній, рейтингами генеральних директорів, інтерв'ю та запитаннями, звітами про зарплату, оглядами виплат, фотографіями офісу тощо.

Glassdoor також є корисним веб-інструментом конкурентної розвідки, оскільки він дає відповіді на такі питання як «Чому людям подобається працювати на цих підприємствах?», «Що кажуть працівники конкурентів?» тощо.

15. Crunchbase – платформа для пошуку бізнес-інформації.

Crunchbase – це одна з найкращих та найбільш інноваційних платформ для пошуку бізнес-інформації про приватні та державні компанії.

Дані основної бази даних включають в себе інформацію про інвестиції та фінансування, новини та тенденції в галузі, осіб на керівних посадах, злиття підприємств тощо.

Приклади того, що можна зробити з Crunchbase: слідкувати за підприємствами, отримати доступ до даних компанії, таким як інформація веб-трафіку та аналітика мобільних додатків.

16. Follow – моніторинг конкурентів.

Follow – це веб-інструмент конкурентної розвідки, який дозволяє отримувати результати аналітичної обробки даних про будь-який веб-сайт. Понад 30000 людей використовують його для отримання цінних конкурентних знань, які допомагають приймати кращі бізнес-рішення.

Follow дає можливість ознайомитися з узагальненим оглядом будь-якого сайту, включаючи оцінку трафіку, оптимізацію пошукових систем, пошуковий маркетинг, медійну рекламу, афілійований маркетинг, демографічні показники тощо.

Вони поєднують у собі декілька джерел для отримання розширеного і високоякісного огляду даних будь-якого сайту.

17. Prisync – це програмний інструмент для відстеження цін конкурентів для підприємств усіх розмірів та типів.

Інформація про ціни конкурентів має вирішальне значення на динамічному ринку сьогодення, і завдяки цьому Prisync стає таємною зброєю на ринковому середовищі.

Prisync – надзвичайно зручний і має автоматизований спосіб збору інформації про конкурентні ціни. Це дозволяє аналізувати ціни конкурентів, щоб придумати розумну стратегію конкурентоспроможності та ціноутворення [46].

4.3 Рекомендації щодо застосування методів конкурентної розвідки у контексті забезпечення інформаційної безпеки підприємства

На основі вивчення теоретичних та практичних засад впровадження конкурентної розвідки як засобу інформаційно-аналітичного супроводу бізнес-діяльності доцільно виділити низку рекомендацій, дотримання яких сприятиме захисту інтересів підприємства в інформаційній сфері, покращенню заходів забезпечення інформаційної безпеки і, як наслідок – створенню системи ефективного управління та підвищенню конкурентоспроможності компанії на ринку.

Рекомендації

1. З метою забезпечення інформаційної безпеки підприємства конкурентна розвідка має виконувати такі завдання, як:

- інформаційне забезпечення процесу вироблення управлінських рішень;
- «система раннього попередження», прийняття рішень щодо загроз;
- виявлення сприятливих можливостей для бізнесу;
- виявлення спроб конкурентів отримати доступ до закритої інформації;
- управління ризиками для швидкого реагування компанії на зміни у навколишньому середовищі;
- промислова контррозвідка, запобігання розвідувальній діяльності конкурентів.

2. У процесі розвідувальної діяльності варто дотримуватися таких основних принципів: об’єктивності, єдності теорії та практики, спрямування розвідувальної роботи на розвиток бізнесу, а також забезпечення автентичності діяльності, дотримання всіх формальних домовленостей та угод, дотримання всіх прав та законів інтелектуальної власності, здійснення постійного моніторингу роботи консультантів.

3. На практиці варто використовувати увесь наявний арсенал методів конкурентної розвідки, зокрема методи альтернативних ресурсів, аналізу можливості, дивергенції, фактичного аналізу й аналізу конкурентних гіпотез, ідентифікації проблем, контр-аналітичний метод.

4. У залежності від таких факторів, наприклад, як розмір та вид діяльності компанії, функція конкурентної розвідки може забезпечуватися різними суб'єктами всередині або поза межами підприємства: керівництвом компанії (командою), професійним підрозділом з конкурентної розвідки; зовнішньою організацією (аутсорсом), яка підписала контракт з компанією; командою компанії під керівництвом фахівця з конкурентної розвідки від зовнішньої організації.

5. При впровадженні програми конкурентної розвідки на підприємстві визначаються наступні складові:

- інтеграція та підготовка методичних процедур;
- встановлення цілей або показників для оцінки результатів;
- здійснення проектів чи досліджень у конкурентному середовищі;
- розробка та впровадження порядку виконання заходів щодо впровадження результатів проектів чи досліджень;
- забезпечення механізму зворотного зв'язку;
- визначення форм можливої співпраці із зовнішніми організаціями.

6. На думку фахівців, процес впровадження конкурентної розвідки на підприємстві має складатися з трьох основних фаз, які поділяються на етапи:

- Управлінська підготовка до впровадження конкурентної розвідки
  - ознайомлення керівництва з сутністю КР;
  - рішення про впровадження КР;
  - визначення форм реалізації та функціонування КР;
  - встановлення особи, відповідальної за виконання і призначені функції.
- Особисто-орієнтована та професійна підготовка до застосування конкурентної розвідки
  - перегляд особистих якостей працівників в команді КР;
  - підбір кваліфікованого персоналу;
  - навчання відібраних осіб методології КР.
- Організаційна підготовка до впровадження та застосування конкурентної розвідки

- порядок розподілу завдань;
- призначення керівника групи КР;
- порядок завершення завдань;
- система класифікації працівників;
- система заохочення співробітників підрозділу КР.

7. Обов’язковою складовою діяльності конкурентної розвідки на підприємстві має бути контррозвідка як інструмент реалізації оборонної тактики і протидії розвідувальній діяльності конкурентів. Активними компонентами корпоративної контррозвідки є: корпоративні розслідування, конкурентні розвідувальні та контррозвідувальні операції, колективний етичний процес; пасивними - формування ситуаційної обізнаності персоналу щодо загроз шпигунства, захисні заходи, технічні контрспостереження, тестування на проникнення.

Висновки до четвертого розділу

Для потреб конкурентної розвідки зі збору та обробки інформації в мережі Інтернет використовують різноманітні інструменти, починаючи з засобів пошуку інформації на окремих сайтах, підбірок посилань, каталогів, пошукових та метапошукових систем, закінчуючи багатофункціональними системами моніторингу і контент-аналізу, екстракторами об'єктів, подій і фактів, системами пошуку знань.

Серед найкращих пошукових систем на кінець 2019 року відзначають: Google, Baidu, Yahoo!, Yandex та Bing. Їх вважають кращими завдяки ефективній системі веб-майнінгу, який включає засоби, що забезпечують аналіз контенту, структур та статистики відвідування.

Для спеціалістів з конкурентної розвідки сьогодення розробляються програмне забезпечення й додатки для розширених досліджень ринку, які спрямовані зокрема на розвідку соціальних мереж, моніторинг контенту та відстеження трафіку конкурентів. Деякі інструменти надають допомогу для здійснення більш глибокого і якісного вивчення ринку. Не використання таких

інструментів конкурентної розвідки у нас час для фахових спеціалістів означає величезну втрату часу і зайву роботу.

На основі дослідження визначено основні рекомендації щодо використання методів конкурентної розвідки на підприємстві, серед яких виділено такі: 1) спрямування конкурентної діяльності на виконання завдань інформаційного забезпечення процесу вироблення управлінських рішень, виконання функції «системи раннього попередження», виявлення сприятливих можливостей для бізнесу та спроб конкурентів отримати доступ до закритої інформації, управління ризиками, ведення контррозвідки; 2) дотримання принципів розвідувальної діяльності (об'єктивності, єдності теорії та практики, спрямування розвідувальної роботи на розвиток бізнесу, дотримання нормативних вимог та угод, здійснення нагляду за роботою консультантів; 3) використання в роботи усього різноманіття методів конкурентної розвідки; 4) усвідомлений вибір суб'єктів реалізації функцій конкурентної розвідки всередині або поза межами підприємства; 5) впровадження програми конкурентної розвідки на підприємстві відповідно до представленої схеми; 6) організація процесу впровадження конкурентної розвідки на підприємстві має складатися з трьох основних фаз: управлінської, особисто-орієнтованої та професійної підготовки; 8) ведення контррозвідки з метою протидії розвідувальній діяльності конкурентів.

ВИСНОВКИ

У результаті дослідження встановлено, що ЗІБ підприємства має на меті створення умов для збереження цілісності, повноти й точності інформації, мінімізація ризику несанкціонованих змін у корпоративних ІТКС. Систему ЗІБ підприємства визначено як сукупність організаційних, нормативних, технічних, програмних заходів, які впроваджуються у контексті вимог бізнесу з метою гарантувати стан захищеності інтересів компанії в інформаційній сфері.

З'ясовано, що в нинішніх умовах збільшення ролі інформації та ІТ у бізнес-сфері конкурентна боротьба між суб'єктами підприємництва переходить в інформаційну сферу. Для ЗІБ підприємства необхідним є комплексний підхід, який включає не тільки захист інформаційних ресурсів та інфраструктури підприємства, запобігання несанкціонованим діям з інформацією та забезпечення її конфіденційності, але й інформаційне забезпечення підприємницької діяльності.

Успішне ЗІБ сучасного підприємства є неможливим без здійснення цілеспрямованої, послідовної та кваліфікованої діяльності зі збору, обробки інформації з важливих питань життєдіяльності суб'єкта підприємництва та інформування керівництва з метою прийняття оптимальних управлінських рішень. У нинішніх умовах основний перелік завдань з інформаційно-аналітичного ЗІБ підприємства виконує конкурентна розвідка.

Конкурентна розвідка – є легальним процесом ідентифікації, збору, оцінки та поширення інформації про сильні та слабкі сторони конкурента, а також інформацію про продукти та споживачів. Підприємства використовують конкурентну розвідку для того, щоб забезпечити надійний захист економічної та інформаційної безпеки і покращити свої позиції на ринку.

Серед основних методів конкурентної розвідки варто відзначити: метод альтернативних ресурсів; метод аналізу можливості; контр-аналітичний метод; метод дивергенції; методи фактичного аналізу та аналізу конкурентних гіпотез; метод ідентифікації проблем тощо. Загалом у конкурентній розвідці використовують кілька десятків аналітичних методів.

З'ясовано, що процес реалізації конкурентної розвідки на підприємстві складається з трьох етапів, якими є: підготовка керівника до впровадження

конкурентної розвідки; особово-орієнтована та професійна підготовка до застосування конкурентної розвідки; організаційна підготовка до впровадження та застосування конкурентної розвідки.

Однією зі складових конкурентної розвідки на підприємстві є контррозвідка, яка має на меті виявлення та нейтралізацію численних загроз, які створюють спецслужби будь-яких конкурентів, та маніпулювання цими службами на користь маніпулятора. Класичний процес контррозвідки на всіх рівнях включає чотири етапи, серед яких: оцінка контррозвідувального захисту; проведення контррозвідувальних спостережень; розробка плану контррозвідки; здійснення відповідних контррозвідувальних заходів.

Для потреб конкурентної розвідки зі збору та обробки інформації в мережі Інтернет використовують різноманітні інструменти, починаючи з засобів пошуку інформації на окремих сайтах, підбірок посилань, каталогів, пошукових та метапошукових систем, закінчуючи багатофункціональними системами моніторингу і контент-аналізу, екстракторами об'єктів, подій і фактів, системами пошуку знань.

Також для потреб конкурентної розвідки розробляється програмне забезпечення й додатки, які забезпечують проведення розширених досліджень ринку, зокрема розвідки соціальних мереж, моніторингу контенту та відстеження трафіку конкурентів. Використання таких інструментів дозволяє фахівцям конкурентної розвідки зекономити величезну кількість часу і уникнути зайвої пошукової та аналітичної роботи.

За підсумками дослідження визначено основні рекомендації щодо використання методів конкурентної розвідки на підприємстві, серед яких виділено такі: 1) спрямування конкурентної діяльності на виконання завдань інформаційного забезпечення процесу вироблення управлінських рішень, виконання функції «системи раннього попередження», виявлення сприятливих можливостей для бізнесу та спроб конкурентів отримати доступ до закритої інформації, управління ризиками, ведення контррозвідки; 2) дотримання принципів розвідувальної діяльності (об’єктивності, єдності теорії та практики,

спрямування розвідувальної роботи на розвиток бізнесу, дотримання нормативних вимог та угод, здійснення нагляду за роботою консультантів; 3) використання в роботи усього різноманіття методів конкурентної розвідки; 4) усвідомлений вибір суб'єктів реалізації функцій конкурентної розвідки всередині або поза межами підприємства; 5) впровадження програми конкурентної розвідки на підприємстві відповідно до представленої схеми; 6) організація процесу впровадження конкурентної розвідки на підприємстві має складатися з трьох основних фаз: управлінської, особисто-орієнтованої та професійної підготовки; 8) ведення контррозвідки з метою протидії розвідувальній діяльності конкурентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ткачук Т.Ю. Конкурентна розвідка : навч. посіб. / Т.Ю.Ткачук. – К. : 2013. – 295 с.

2. Бурцева К., Тимофєєв Д. Підвищення рівня інформаційної безпеки за допомогою організаційних заходів на комерційних підприємствах. [Електронний ресурс]. – Режим доступу: http://ir.nmu.org.ua/bitstream/handle/123456789/1673/6.pdf?sequence=1

3. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. - М.: ИНФРА-М, 2001. - 304 с.

4. Мельник С., Цуп М. Інформаційна безпека як складова економічної безпеки підприємства. [Електронний ресурс]. – Режим доступу: http://nauka.kushnir.mk.ua/?p=66146

5. Ярочкин В. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.

6. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002 – 688 с.

7. Методи конкурентної розвідки. [Електронний ресурс]. – Режим доступу: http://alt.ck.ua/3-metody-biznes-rozvidky-konkurentiv/

8. Ортинський В. Л. Економічна безпека підприємств, організацій та установ: Навч. посібник /для студ. вищ. навч. закл.], І. С. Керницький, З. Б. Живко та ін. Київ: Правова єдність, 2009 . – 542 с.

9. Березюк Л. Организационное обеспечение информационной безопасности: учеб. пособие / Л.П. Березюк. - Хабаровск : Изд-во ДВГУПС, 2008. - 188 с.

10. Романов О. Организационное обеспечение информационной безопасности: Учеб. пособие. - М.: Издательский центр «Академия», 2008. – 192 с.

11. Управление информационной безопасностью. [Електронний ресурс]. – Режим доступу: http://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html

12. Whitman, M. E., Mattord, H. J.Management of Information Security. [Електронний ресурс]. Режим доступу: https://ru.scribd.com/doc/102088851/Management-of-Information-Security

13. Манойло А.В. Государственная информационная политика в особых условиях: Монография. М.: МИФИ, 2003. – 388 с. [Електронний ресурс]. – Режим доступу: http://www.evartist.narod.ru/text24/0022.htm

14. Ліпкан В.А. Національна безпека України: Навчальний посібник. 2-ге в. / В.А. Ліпкан. — К.: КНТ, 2009. — 576 с.

15. Ковальчик Я. Конкурентна розвідка в управлінні конкурентною поведінкою підприємства // Управління конкурентоспроможністю: теорія і практика Під ред. Е.Горбашко, І.Максимцева. [Електронний ресурс]. – Режим доступу: http://stud.com.ua/43060/ekonomika/ekonomichna_povedinka_pidpriyemstva_zabezpechennyu_konkurentospromozhnosti#74

16. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 - 216 с.

17. Чергенець Е.В., Зайцев А.В., Позднишев Є.В. Інформаційно-аналітичне забезпечення безпеки підприємництва (збір та пошук інформації). Навч. посібник. Книга 2. / Під заг. ред. Є.В.Позднишева. - К., Видавець Позднишев, 2007. - 74с.

18. Techopedia. Competitive Intelligence. URL: https://www.techopedia.com/definition/28534/competitive-intelligence-ci (дата звернення 07.04.2018).

19. Fuld + Company. What is Competitive Intelligence? URL: http://www.fuld.com/what-is-competitive-intelligence (дата звернення 07.04.2018).

20. Competitive Analytics. Competitive Intelligence. URL: http://competitiveanalytics.com/competitive-intelligence/ (дата звернення 14.04.2018).

21. J. J. McGonagle. Proactive Intelligence. What is Competitive Intelligence and Why Should You Care about it? / J.J. McGonagle, C.M. Vella. Springer-Verlag London, 2012. P. 9–19. DOI: 10.1007/978-1-4471-2742-0_2.

22. Цирфа Г.О. Забезпечення інформаційної безпеки у конкурентних відносинах: розвідка і промислове шпигунство. *Інформація і право*. 2015. № 3 (15). С. 66-71.

23. Business Jargons. Competitive Intelligence. URL: https://businessjargons.com/competitive-intelligence.html (дата звернення 14.04.2018).

24. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. – К.: ИПРИ НАН Украины, 2013. – 250 с., Подоляк О.О. Конкурентная разведка. Учебное пособие / О. О. Подоляк, Е. Ю. Кузнецова. Екатеринбург: УрФУ, – 2012. – 93 с.

25. Hartmann, Blackmon & Kilgore P.C. Four principles of competitive intelligence. 2017. URL: https://www.hbkcpas.net/4-principles-of-competitive-intelligence/ (дата звернення 21.04.2018).

26. F. Bartes. The objectives of competitive intelligence as a part of corporative development strategy. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis. 2014. Volume 62. №6. P. 1243–1250.

27. V. Gaidelys. Economics and management. Instruments and methods of competitive intelligence. 2012. №17 (3). P. 971–977. ISSN 2029-9338.

28. E. Metayer. 50 Competitive Intelligence Analysis Techniques. 2013. URL: http://competia.com/50-competitive-intelligence-analysis-techniques

29. F. Bartes. Intelligence analysis – the royal discipline of Competitive Intelligence. 2011.

30. A. Kocmanova, M. Docekalova. Environmental, Social, and Economic Performance and Sustainability in SMEs. 2011.

31. F. Bartes. Competitive intelligence – tool obtaining specific basic for strategic decision making TOP management firm.

32. J. Herring. KITs Revisited: Their Use and Problems. 2006

33. J.E. Prescott, S.H. Miller. Proven Strategies in Competitive Intelligence: Lessons from the Trenches. 2001

34. V. Dostal, J. Loubal, F. Bartes. *Hodnotové inženýrství. Cesta k dosažení komerčně úspěšného výrobku.* Ostrava: KEY Publishing, 375 s. ISBN 978-80-7418-003-3.

35. L.M. Fuld. The New Competitor Intelligence. 1995.

36. D. Bernhardt. Competitive Intelligence: How to acquire and use corporate intelligence and counter-intelligence. 2003.

37. K.G. Strauss. Marketing Telecommunication Services. 1999.

38. U.S. Marine Corps. Counterintelligence. 2007.

39. Unfair Competition. 2019 [URL: https://www.encyclopedia.com/law/encyclopedias-almanacs-transcripts-and-maps/unfair-competition-0]

40. Tara. The 5 Main Types of Unfair Competition. [URL: https://primumlaw.com/2017/10/20/5-main-types-unfair-competition/]

41. Manish Khanna. 2018. [URL: https://www.smallbusinessbonfire.com/unethical-business-practices/]

42. H. Chen, M.I. Chau, D. Zebg. CI Spider: A Tool for Competitive Intelligence on the Web. 2002.

43. M.H. Dunham. Data Mining: Introductory and Advanced Topics. 2003.

44. L. Page, S. Brin, The Anatomy of a Large-Scale Hypertextual Web Search Engine. 1998

45. J.M. Kleinberg. Authoritative Sources in a Hyperlinked Environment. 1999.

46. S. Valcheva. 50 Best Web Competitive Intelligence Tools and Techniques. [URL: intellspot.com/web-competitive-intelligence/]

47. H. Friedman. The 32 Best Competitive Intelligence Companies. 2019. [URL: improvado.io/blog/32-best-competitive-intelligence-companies]