Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України

Відкритий міжнародний університет розвитку людини “Україна”

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 2(33)/2020

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 20117-9917ПР від 05.07.13 р.).

Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12),
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів кандидата наук (доктора філософії – Ph.D.)
і доктора наук у галузі юридичних наук.
Друковане періодичне видання ІНФОРМАЦІЯ І ПРАВО внесене в міжнародну базу даних
періодичних видань, згідно відповідного номеру ISSN.

м. Київ

З М І С Т

Інформаційне право

ДЗЬОБАНЬ О.П., ЖДАНЕНКО С.Б. Права людини і національна безпека: філософсько-правові аспекти взаємозв'язку……..….. **9**

КОСІЛОВА О.І. Тлумачення статті 21 Конституції України у контексті європейської правової доктрини…….…… **23**

ЛЕОНОВ Б.Д., ЧУМАК Л.А., ГРИНЕНКО С.В. Проблеми запобігання сексуальній експлуатації дітей в мережі Інтернет: досвід ЄС…..... **32**

УХАНОВА Н.С. Особливості захисту прав неповнолітніх в інформаційному просторі…….…….…..... **40**

Правова інформатика

ЛАНДЕ Д.В. Правові питання конкурентної розвідки…..... **51**

БРАЙЧЕВСЬКИЙ С.М. Проблема персональних даних при використанні систем Інтернету речей в галузі охорони здоров'я……... **69**

Інформаційна і національна безпека

МАРУЩАК А.І., ПЕТРОВ С.Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України). **77**

ДОВГАНЬ О.Д., ТАРАСЮК А.В. Протидія загрозам кібербезпеці держави на глобальному рівні..... **85**

ХАХАНОВСЬКИЙ В.Г., ГАВЛОВСЬКИЙ В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів…..... **99**

СТРЕЛЬБИЦЬКА Л.М., СТРЕЛЬБИЦЬКИЙ М.П. Методологічні та організаційно-правові засади формування і функціонування системи державного управління національною безпекою України……..……..... **110**

БАТИРГАРЕЄВА В.С. Основні напрями протидії поширенню дезінформації (на прикладі пандемії CoVID-19)……..... **121**

МАЄВСЬКИЙ О.О. Формування інформаційного простору в так званих "ДНР" та "ЛНР" методами експлуатації візуальних образів Другої світової війни……..…….…..... **132**

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

ЯЩЕНКО В.А. Військове право: теоретико-методологічні засади……... **141**

КОРЖ І.Ф. Трансформація суспільних відносин у процесі утворенням об'єднаних територіальних громад…….. **149**

Правова інформатика

УДК 316.324.8

ЛАНДЕ Д.В., *доктор технічних наук, професор,* керівник наукового центру НДІ інформатики і права НАПрН України.

ПРАВОВІ ПИТАННЯ КОНКУРЕНТНОЇ РОЗВІДКИ

Анотація. *У статті викладені правові засади конкурентної розвідки, опис її ролі і місця в сучасному суспільстві, сфер її застосування, стану відповідного правового забезпечення в Україні та світі. Досліджуються основні проблемні питання, пов'язані з керуванням репутацією, захистом комерційної таємниці, персональних даних, авторських прав і суміжних питань. Обґрунтовано актуальність конкурентної розвідки, яка пов'язана з такими процесами, як глобалізація економіки, зростання конкуренції, цифровізація, віртуалізація економіки, розвиток інформаційних технологій. Визначено, що застосування та подальший розвиток правових аспектів конкурентної розвідки може стати важливою ланкою формування сучасного бізнес-середовища.*

Ключові слова: *конкурентна розвідка, захист комерційної таємниці, захист персональних даних, керування репутацією в мережах, OSINT, відкриті джерела інформації.*

Summary. *The article is devoted to the legal aspects of competitive intelligence, a description of its role and place in modern society, its application areas, the state of the relevant legal support in Ukraine and the world. The main problematic issues related to reputation management, protection of trade secrets, personal data, copyrights and related issues are investigated. The relevance of competitive intelligence, which is associated with processes such as globalization of the economy, increasing competition, digitalization, virtualization of the economy, the development of information technology, is substantiated.*

It is determined that the application and further development of the legal aspects of competitive intelligence can become an important link in the formation of the modern business environment.

Keywords: *competitive intelligence, commercial secrets protection, personal data protection, reputation management in networks, OSINT, open information sources.*

Аннотация. *В статье изложены правовые основы конкурентной разведки, описанию ее роли и места в современном обществе, сферам ее применения, состояния соответствующего правового обеспечения в Украине и мире. Исследуются основные проблемные вопросы, связанные с управлением репутацией, защитой коммерческой тайны, персональных данных, авторских прав и смежных вопросов. Обоснована актуальность конкурентной разведки, которая связанна с такими процессами, как глобализация экономики, рост конкуренции, цифровизация, виртуализация экономики, развитие информационных технологий. Определено, что применение и дальнейшее развитие правовых аспектов конкурентной разведки может стать важным звеном формирования современной бизнес-среды.*

Ключевые слова: *конкурентная разведка, защита коммерческой тайны, защита персональных данных, управление репутацией в сетях, OSINT, открытые источники информации.*

Постановка проблеми. Конкурентна розвідка (Competitive Intelligence) охоплює процедури збору і обробки інформації, що проводяться з метою підтримки прийняття управлінських рішень, підвищення конкурентоспроможності комерційних організацій, виключно з відкритих джерел з комп'ютерних мереж [1], більшість з яких є так званими

оверлейними, тобто надбудованими над мережею Інтернет, найпоширеніші з яких – соціальні мережі.

Основна відмінність конкурентної розвідки від бізнес-розвідки в широкому розумінні, в тому числі і від промислового шпигунства – це легітимність і дотримання етичних норм [2]. У конкурентній розвідці це положення доведено до абсолюту – виключно всі джерела інформації повинні бути доступними і легальними.

Очевидно, таке глобальне поняття як конкурентна розвідка вимагає чіткого визначення її легітимних рамок, сфер застосування, правових засад, – цим питанням присвячена ця стаття.

Застосування конкурентної розвідки в комерційній компанії не може бути виправдане тільки міркуваннями інформаційної безпеки, але важливо і для вирішення завдань менеджменту і маркетингу тим, що забезпечує:

- спостереження за репутацією компанії;
- активна участь у формуванні іміджу компанії, інформаційного поля навколо компанії;
- відстеження появи нового конкурента, технології або каналу збуту;
- виявлення можливих злиттів і поглинань;
- оцінка потенційних ризиків при інвестиціях;
- випередження кроків конкурентів в рамках маркетингових кампаній;
- випередження конкурентів в тендерах;
- виявлення каналів витоку інформації.

Хитка грань між поняттями “конкурентна розвідка” і “промислове шпигунство”, полягає в легітимності, законності методів і засобів, що використовуються в процесі збору цільової інформації [3]. Слід зазначити також вельми тонку різницю між бізнес-розвідкою (Business Intelligence) і конкурентною розвідкою. З публікацій і описів систем, де згадуються ці терміни, можна зробити висновок, що бізнес-розвідка спрямована більше на вивчення “внутрішньої” маркетингової, фінансової, економічної інформації та інформації про клієнтів, в той час як конкурентна розвідка частіше охоплює процеси, пов’язані з добуванням “зовнішньої” інформації і знань безпосередньо про конкурентів.

Родоначальником сучасної конкурентної розвідки вважається компанія “Ксерокс”, що зіштовхнулася з конкуренцією з боку японських виробників. У той час японці вийшли на американський ринок з роздрібними цінами нижче собівартості “Ксерокса”. Але “Ксерокс”, завдяки своїй японській філії, створив систему роботи, яку сьогодні називають бенчмаркингом, засновану на аналізі інформації з відкритих джерел, і отримав успіх.

Приклад нехтування інформації із відкритих джерел. У 70-х роках XX століття “Велика трійка” американських виробників автомобілів не прореагувала на появу на ринку японських виробників автомобілів. Однак, самі американці обрали невеликі, економічні і надійні японські автомобілі, і американські корпорації зазнали значних збитків.

Компанія AT & T повідомляла, що в неї існує система моніторингу питань, пов’язаних з напрямками діяльності цієї фірми, якими цікавляться співробітники AT & T, що працюють в різних регіонах світу. В результаті одного разу новий великий конкурент по одному з видів діяльності AT & T був виявлений за місяць до того, як публікації про нього з’явилися у світовій діловій пресі.

В арсеналі тих, хто сьогодні займається конкурентною розвідкою, немає шпигунської техніки. Їх основний інструмент – комп’ютер, підключений до мережі Інтернет, іноді мережевий доступ до спеціальних агрегаторів інформації. Діяльність

сучасних підрозділів конкурентної розвідки компаній часто ґрунтується на останніх досягненнях в області штучного інтелекту, обробки "Великих даних" (Big Data) в поєднанні з напрацюваннями в сферах психології, соціології, економіки.

У цей час створюються численні професійні об'єднання (спільноти) фахівців в галузі конкурентної розвідки. Найбільш відомі з таких спільнот, що займаються організацією конференцій, тренінгів, – це Strategic and Competitive Intelligence Professionals, SCIP (//www.scip.org) в США і Competia (//www.competia.com) в Канаді.

В Україні відома громадська організація "Спільнота аналітиків і професіоналів конкурентної розвідки" (https://www.scip.org.ua). Також ведеться підготовка фахівців в області конкурентної розвідки в Харківському національному університеті радіоелектроніки, де готують магістрів за спеціальністю "Консолідована інформація".

З початком російської агресії щодо України питання отримання інформації з відкритих джерел і розвінчання фейків отримало нове звучання. Це призвело до старту нових проектів і навчальних платформ, метою яких стало формування і поширення навичок і умінь працювати з інформацією он-лайн, перевіряти інформацію і т.д. Серед таких проектів можна назвати OSINT Academy, сервіс Attack Index (http://attackindex.com) і безкоштовний он-лайн курс по OSINT Інституту постіндустріального суспільства [4].

Метою статті є опис поняття конкурентної розвідки, її ролі та місця в сучасному суспільстві в умовах цифровізації, сфер її застосування, дослідження стану відповідного правового забезпечення в Україні та світі, зокрема, основних проблемних питань, пов'язаних із захистом комерційної таємниці, персональних даних, керування репутацією, авторських прав та суміжних питань.

Виклад основного матеріалу

Конкурентна розвідка і OSINT. Методи ведення конкурентної розвідки, техніки і технології її проведення дуже близькі до тих, що використовуються в традиційній розвідувальній діяльності спецслужбами. В англомовній літературі такий вид конкурентної розвідки прийнято називати розвідкою за відкритими джерелами (Open Sources INTelligence, OSINT) [5]. Однак слід зазначити, що OSINT значною мірою обмежена застосуванням у державній, військовій, правоохоронній сфері. Але саме для технологій OSINT створено найбільшу кількість методик, технік, технологій [6; 4; 7].

Комерційна інформація може бути отримана з офіційних джерел, засобів масової інформації, оголошень, реклами, внутрішніх фірмових, банківських, урядових звітів, баз даних, від експертів, шляхом збору, аналізу або спеціальної обробки даних. Відомо, що для бізнес-структур 95 % корисної інформації дає конкурентна розвідка, 4,1 % інформації можна легально отримати від державних структур. Правда, при цьому кількість різнорідних відомостей, які необхідно переробити, щоб отримати крупиці знань, величезна, а тому в даний час конкурентна розвідка немислима без використання спеціалізованих інформаційних технологій, практичного застосування сучасної концепції "Великих даних".

Дозволити собі проведення повнофункціональної бізнес-розвідки на ринках можуть тільки великі компанії, проте можливості конкурентної розвідки доступні практично всім.

Значимість розвідки за відкритими джерелами зазначив ще президент США Ліндон Джонсон (Lyndon Baines Johnson) 30 червня 1966 р., коли виголосив промову на церемонії прийняття присяги директором ЦРУ Річардом М. Хелмсом (Richard McGarrah Helms): "Вищі досягнення не є результатом потихеньку переказаної таємної інформації, а випливають з терплячого, повсякчасного вивчення друкованих джерел".

За твердженнями аналітика ЦРУ Шермана Кента у 1947 р., політики отримують з відкритих джерел до 80 % інформації, необхідної їм для прийняття рішень в мирний час. Пізніше генерал-лейтенант С. Вілсон, який був керівником РУМО США в 1976 – 1977 роках, зазначав, що "90 відсотків розвідданих приходить з відкритих джерел і тільки 10 – за рахунок роботи агентури" [8; 9].

У той же час, аналіз розсекреченого звіту ЦРУ за 1987 рік "Enterprise-Level Computing in Soviet Economy" (SOV C87-10043) дає уявлення про те, який колосальний обсяг даних необхідно було обробляти аналітикам. Для складання звіту постійно протягом року сканували 347 відкритих джерел; для створення зведення обсягом в одну сторінку щодня оброблявся інформаційний масив обсягом приблизно 7 млн. слів.

На державному рівні в США основним правовим механізмом ведення розвідки в відкритих джерелах міністерства оборони є Рада із захисту відкритих джерел (DOSC).

Ця рада консультує і доповідає заступнику міністра оборони з розвідки про питання ведення розвідки в відкритих джерелах, про нові ініціативи щодо поліпшення ефективності роботи підрозділу OSINT і діяльності міністерства оборони в цілому.

В обов'язки ради входять: координація діяльності підрозділу OSINT і ствердження його плану ведення розвідки в відкритих джерелах; визначення послідовності вимог до процесу ведення розвідки в відкритих джерелах.

Армійський стандарт США "ATP 2-22.9" встановлює загальні поняття, основні концепції та методи збору розвідувальних даних з відкритих джерел для Армії США. У цьому документі підкреслюється характеристика OSINT як розвідувальної дисципліни, його зв'язку з іншими розвідувальними дисциплінами, і можливості його застосування в ході спільних операцій.

Використання загальнодоступної інформації є важливим аспектом технічної розвідки (TECHINT). Незважаючи на те, що наміри, можливості і чинники уразливості супротивників і потенційних загроз підлягають засекречуванню, результати OSINT (зокрема, відкритого сервісу "Google Earth") сприяють отриманню інформації про найбільш потайні держави і організації. Такі приклади свідчать про відповідальність діяльності в цій галузі.

Модель предметної області "Конкурентна розвідка". Під моделлю предметної області, зокрема, розуміють спеціальним чином сформовану мережу понять, онтологію. Побудова онтології – складна проблема. Перший етап цього процесу – побудова термінологічної основи онтології і визначення семантичних зв'язків.

Нами застосовується методика побудови інформаційних мереж – моделей предметних областей на основі автоматичного моніторингу і аналізу мережевих інформаційних ресурсів довідкового характеру [10]. Як така мережа розглядається мережа понять, що відповідають термінам-заголовкам статей мережевої енциклопедії Wikipedia, що є доступною в мережі Інтернет і не передбачає передплати, крім того, доступна для завантаження у повному обсязі. Для первинного доступу до системи застосовано спеціальний термін Competitive Intelligence (Конкурентна розвідка), за яким існують відповідні статті, що створюються і редагуються експертами-авторами (Рис. 1).

Застосовувався наступний алгоритм побудови моделей предметних областей за даними сервісу Wikipedia [11]:

1. Обирається перший термін-поняття, з якого починається зондування.

2. Відкривається сторінка веб-сервісу (стаття Wikipedia), що відповідає обраному терміну-поняттю. До створюваної мережі додаються всі терміни-поняття, що відповідають гіперпосиланням на обраній сторінці. Формуються ребра-зв'язки до цих вузлів з вихідного вузла.

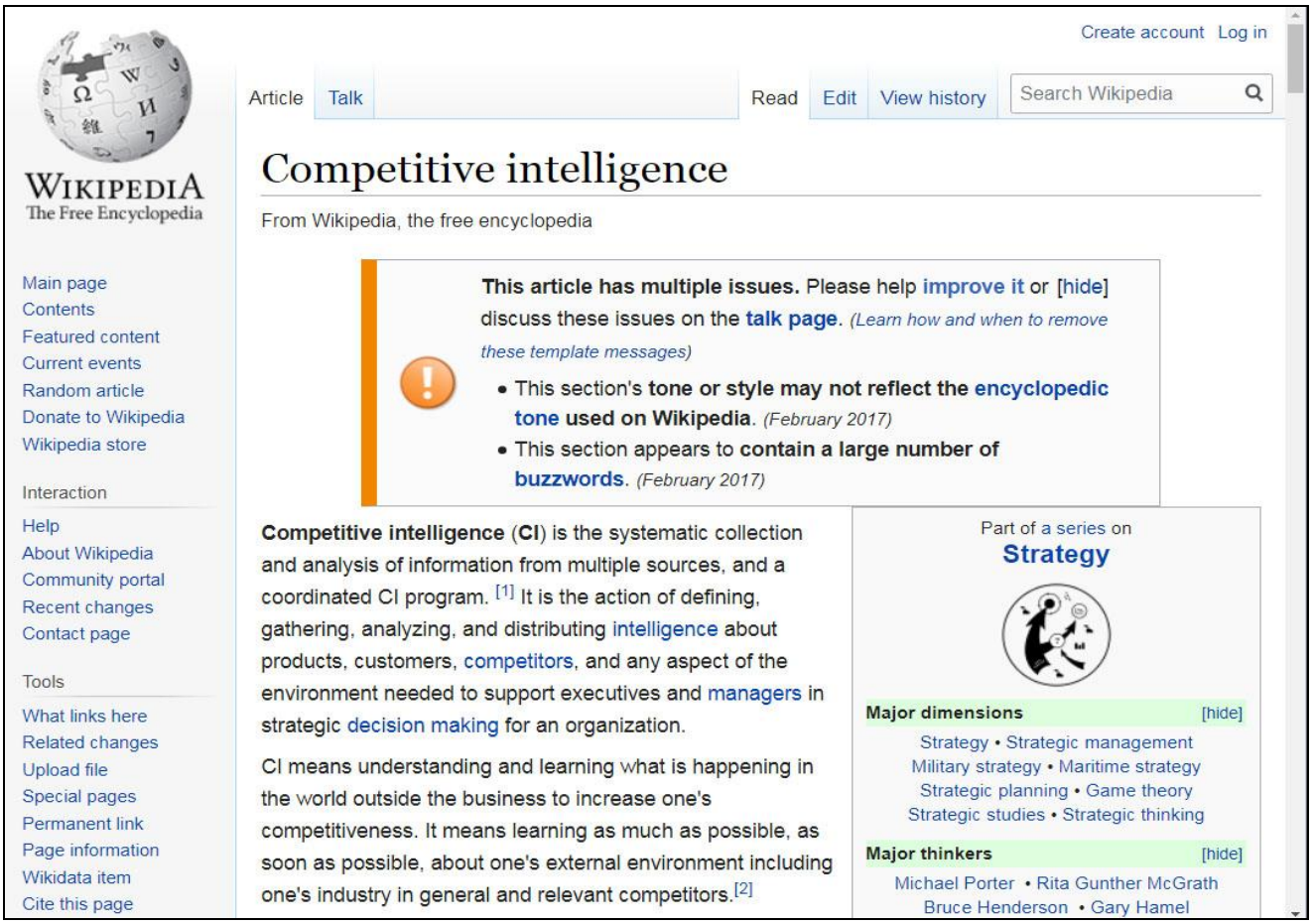

Рис. 1. Інтерфейс користувача системи Wikipedia, розглядається стаття за терміном-поняттям Competitive intelligence

3. Статті, що відповідають гіперпосиланням на попередній сторінці, визначаються як базові, якщо на них міститься гіперпосилання на статтю, що відповідає першому терміну-поняттю, з якого починалось зондування.

4. Із списку вузлів мережі, що формується, визначається той, за яким ще не здійснювалося переходу, на сторінку якого планується перейти для подальшого аналізу. Цей вузол має відповідати вимозі, наведеній у попередньому пункті, та не входить до складу тих вузлів, до сторінок яких вже був здійснений перехід

5. Якщо такий вузол-поняття обрано, то здійснюється перехід до пункту 2.

6. Якщо такого вузла не існує, то вважається, що мережу, що відповідає моделі предметної області, побудовано.

Відповідно до наведеного алгоритму процес збирання інформації з Wikipedia, починаючи з певного вузла-поняття (у нашому випадку – Competitive_intelligence), припиняється, коли відповідно до алгоритму вже неможливий перехід до нового вузла.

Побудовано відповідно до наведеного алгоритму мережі співавторів за базовим терміном-поняттями Competitive intelligence без обмежень на кількість сканованих вузлів. Отримані такі характеристики побудованої мережі: вузлів: 176, зв'язків: 1795, два класи модулярності, дуже висока кластерність: 0.824. Найбільш вагомі за ступенями вузлів поняття наведено у Таблиці 1 (виділені рядки, що містять у словосполученні слово Intelligence).

Таблиця 1. Найбільш вагомі терміни-поняття,
що відповідають поняттю Competitive intelligence

Поняття	Ступень вузла мережі
Industrial_espionage	87
Competitive_intelligence	83
Business_intelligence	75
Strategic_planning	55
University_of_Windsor	50
SWOT_analysis	45
Competitor_analysis	42
Business_war_games	41
Commercial_intelligence	41
Marketing_intelligence	41
Marketing_strategy	41
Society_of_Competitive_Intelligence_Professionals	41
Blindspots_analysis	40
Business_Intelligence	38
Commercial_Intelligence	37
Creative_competitive_intelligence	37
Deformulation	37
Market_intelligence	37
University_of_Windsor_Faculty_of_Human_Kinetics	37
Intelligence_analysis	36
Open_source_intelligence	35
Media_intelligence	34
Mercyhurst_College_Institute_for_Intelligence_Studies	34
Competitor_Intelligence	32
Corporate_planning	32
Deloitte_Consulting	32
OSINT	32
Global_Intelligence_Forum	31
Marketing_management	31
Contify	30
Mercyhurst_University_Institute_for_Intelligence_Studies	30
Marketing_analysis	29
Strategic_and_Competitive_Intelligence_Professionals	29
Marketing_strategies	26

На Рис. 2 показано приклад процесу виявлення кластерів шляхом застосування спеціального алгоритму, що застосовується в системі Gephi.

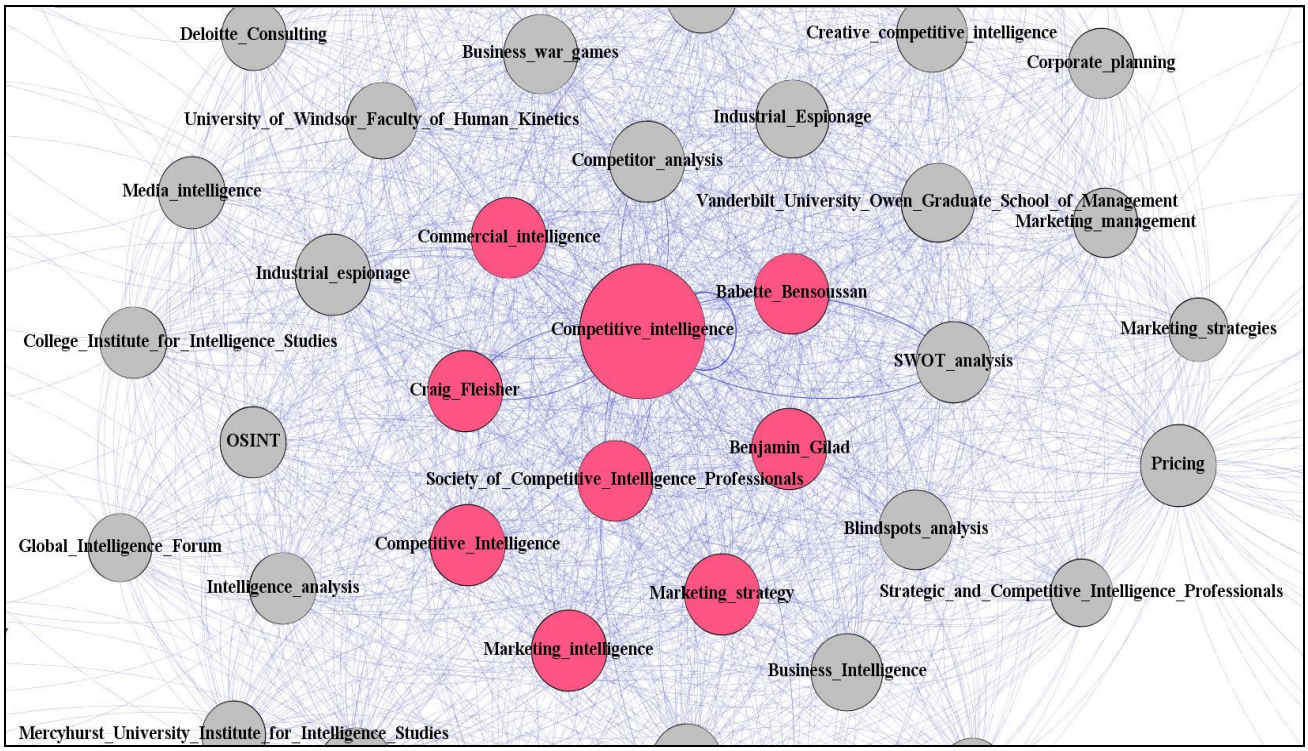

Рис. 2 – Фрагмент моделі предметної області за темою Competitive intelligence

Слід відзначити принципову відмінність запропонованої моделі від існуючих, що базуються на особистій участі експертів при виборі конкретних вузлів і зв'язків. У дослідженні було застосовано лише крупицю знань, представлену у вигляді назви першого, ключового терміну-поняття Competitive_intelligence. Після цього програма екстрагувала знання, закладені авторами (редакторами) статей в Wikipedia.

Таким чином, визначено перелік і рівень суміжних до конкурентної розвідки понять, а саме: Business intelligence, Strategic planning, Industrial espionage, Competitor analysis, Commercial intelligence, Marketing intelligence, Marketing strategy, Business intelligence, Commercial intelligence тощо.

Джерела інформації. В інформаційно-аналітичній роботі головною проблемою є знаходження змістовних і загальнодоступних надійних джерел. Коли такі джерела знайдені, застосовуються відповідні технології. Кінцевим інформаційним продуктом аналітичної роботи є знання – синтезовані висновки, рекомендації для прийняття рішень.

Нижче наведено перелік видів інформаційних джерел, які найчастіше використовуються у конкурентній розвідці [12].

1. Прес-релізи компаній, офіційні заяви від імені компаній про нові технології, нові напрямки, угоди, перспективи. Такі прес-релізи створюються компаніями для власної популяризації, залучення уваги потенційних клієнтів, інвесторів, які шукають вигідні варіанти вкладення своїх коштів. Часто в таких заявах є інформація про наміри, події, що плануються. Прес-релізи доступні на веб-сайтах компаній, в PR-службах, на загальних і профільних спеціалізованих майданчиках.

2. Інтерв'ю співробітників компаній, відповідні матеріали в ЗМІ. В інтерв'ю інтерес представляють плани компаній. При цьому з боку служби конкурентної розвідки допускається ініціювання інтерв'ю когось із співробітників об'єкта інтересу.

3. Висловлювання співробітників компаній на форумах, в блогах, в месенджерах, в приватних бесідах. При цьому можуть виявлятися плани компаній, кадрова політика, атмосфера в колективі і т. п. Джерела інформації: 1) Інтернет-ресурси (спеціалізовані форуми, блоги співробітників), блоги експертів, групи в соціальних мережах, месенджерах; 2) виставки, конференції, курси підвищення кваліфікації, професійні заходи.

4. Тендери, закупівлі. Предмети закупівель, обладнання, виконавці. Джерела інформації: 1) Інтернет-ресурси (веб-сайти компаній, торгові майданчики, профільні форуми); 2) партнери досліджуваної компанії, ті, хто брав участь в їх тендерах, у якостях клієнтів і постачальників.

5. Патенти, авторські свідоцтва компанії і її співробітників. Для завдань конкурентної розвідки цікавий їх зміст, спрямованість, списки співавторів. Інформація розміщується на відповідних сайтах (наприклад, //www.base.ukrpatent.org). Патентування можливо в будь-якій країні, кращі варіанти – країна реєстрації організації, країна ведення бізнесу, крім того США, Євросоюз, Китай.

6. Розробки компанії: розробки, що ведуться, якими компанія цікавиться. Спостереженню підлягають спроби компанії проводити дослідження: закупівля специфічного обладнання, прийом на роботу фахівців, переговори, відвідування відповідних організацій і т.д.

7. Активність компанії на ринку злиття і поглинань (M & A). Інформація про те, які організації поглинаються, планують поглинути або ведуть переговори про поглинання. Інформацію можна отримати в Антимонопольному комітеті України, за новинним повідомленнями на веб-ресурсах, що присвячені M & A.

8. Вакансії компанії (що відкриваються, закриваються), повідомлення про активний пошук співробітників, вимоги до вакансій, умови. Джерело інформації: веб-сайт компанії, сайти з пошуку роботи та сайти агентств, з якими компанія співпрацює.

9. Інтерес представляє те, чого навчають, яких фахівців запрошують для навчання, які вимоги висувають при залученні слухачів і викладачів, які терміни навчання, яка кількість персоналу навчається.

10. Подяки і нагороди компанії та її співробітників.

11. Участь у заходах (виставки, конференції, круглі столи, презентації). З'ясування, в яких заходах беруть участь компанії, їх спрямованість, коло учасників.

12. Участь в організаціях (союзи, асоціації, спільноти і т.п.) – інформація про те, в яких об'єднаннях бере участь компанія, як активно бере участь, що отримує від участі, на що розраховує, як використовує.

Велика частина цих даних потрапляє в мережеву пресу, прес-релізи або публікується на корпоративних веб-сайтах. Останнім часом великої популярності набувають також бази даних на основі архівів мас-медіа, в тому числі (і переважно) мережевих.

Інформація характеризується якісними, кількісними і ціннісними показниками. До якісних характеристик зазвичай відносять: достовірність, об'єктивність і однозначність інформації. До кількісних характеристик – її повноту і релевантність. Ціннісними характеристиками є вартість і актуальність інформації.

Інтернет за кількістю інформації знаходиться на першому місці у світі, випереджаючи ЗМІ, галузеві видання і одержувані від колег новини, спеціальні огляди, закриті бази даних. При цьому у відкритих джерелах міститься велика частина інформації, необхідна для проведення конкурентної розвідки, однак залишається відкритим питання її знаходження і ефективного використання. Останні дослідження

інформаційного простору показали, що через традиційні інформаційно-пошукові системи доступний трильйон веб-сторінок – це лише "поверхнева видима частина айсберга". Близько 40 % всієї інформації в Інтернеті є безкоштовною. Навігацію по даному інформаційному простору забезпечують понад мільйон пошукових систем і каталогів, але й вони охоплюють лише малу частину інформаційних ресурсів. Прихованих і невидимих (deep, invisible) ресурсів мережі Інтернет значно більше – це, перш за все сторінки, що генеруються динамічно, файли різноманітних форматів, інформація з численних баз даних. Сьогодні дуже популярні серед фахівців з конкурентної розвідки бази даних державних і статистичних органів, торговельно-промислових палат, органів приватизації і т.д. Велику користь приносять і окремі доступні бази даних інших органів влади.

Конкурентна розвідка в правовому полі. Конкурентна розвідка як сфера діяльності повинна здійснюватися в рамках правового поля держави. Основою для цього є конституційні права на пошук, отримання, передачу і використання інформації в усіх цивілізованих державах.

Впровадженню систем конкурентної розвідки сприяють законодавчі акти багатьох країн світу. Так, наприклад, в США ще в 1996 році був прийнятий Закон про свободу інформації, який зобов'язав федеральні відомства забезпечити громадянам вільний доступ до всієї своєї інформації. Обмеження стосуються лише матеріалів, що мають відношення до національної оборони, особистих і фінансових документів, а також документів правоохоронних органів.

Однак слід зазначити, що в деяких державах законодавство обмежує подібну діяльність, практично забороняючи конкурентну розвідку.

В Україні "кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір" (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері ґрунтується на наступних принципах:

1) свобода пошуку, отримання, передачі, виробництва і поширення інформації будь-яким законним способом;

2) встановлення обмежень щодо доступу інформації тільки законами держави;

3) відкритість інформації про діяльність державних органів і органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, встановлених законами держави;

4) по категорії доступу інформація поділяється на відкриту (загальнодоступну) і з обмеженим доступом.

Разом з тим, узаконеного поняття "конкурентна розвідка" в Україні сьогодні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів:

Закон України "Про інформацію" від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5 – 7 [13];

Закон України "Про друковані засоби масової інформації (пресу) в Україні" від 16.11.92 р. № 2782-XII, ст. 6, 25 [14];

Закон України "Про охоронну діяльність" від 22.03.12 р. № 4616-VI, ст. 9, 13, 19 [15];

Закон України "Про захист персональних даних" № 2297-VI від 01.06.10 р. [16];

Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163);

Указ Президента України “Питання європейської та євроатлантичної інтеграції” від 20.04.19 р. № 155/2019 [17];

Указ Президента України “Про Національний Координаційний центр кібербезпеки” від 07.06.16 р. № 242/2016 [18].

Не можна забувати, що здійснення заходів щодо забезпечення безпеки бізнесу навіть в рамках конкурентної розвідки іноді може бути сприйнято як проведення оперативно-розшукової діяльності, проводити яку, відповідно до Закону України “Про оперативно-розшукову діяльність” від 18.02.92 р. № 2135-XII [19] можуть лише суб’єкти, зазначені в окремих статтях даних Законів.

У затвердженій Указом Президента України “Стратегії кібербезпеки України” від 15.03.16 р. № 96/2016 [20] декларуються основні завдання силовим органам, а також передбачається “створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій”, все це, безумовно, відноситься до застосування засобів конкурентної розвідки в цій галузі.

У той же час чинним Кримінальним кодексом України передбачено кримінальну відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також за розголошення комерційної таємниці. Однак такі відомості виходять за рамки конкурентної розвідки.

При досить широкому тлумаченні норм законодавства будь-які процедури збору, обробки та зберігання інформації про конкурентів стають, з одного боку, легітимними, практично безкарними, а, з іншого боку, важко доступними. В Україні фактично закритий доступ до великого пласту вільно доступної в більшості країн інформації, наприклад, щодо нерухомості (наявної і закладеної), земельні ділянки, наявність банківських рахунків і т.п. Більшу частину відомостей можна отримати тільки шляхом консультацій з відповідними експертами.

Як ніколи гостро постала проблема криміналізації окремих служб конкурентної розвідки. Багато служб безпеки сьогодні користуються базами даних з інформацією про людину (тобто, про персональні дані). Такі бази використовуються з цілком благими цілями, наприклад, для перевірки даних про співробітників, партнерів і конкурентів. Очевидно, такими базами даних вони будуть користуватися і надалі, проте будуть вимушені порушувати закон і “йти в підпілля”. Технічно можливості використання і ведення подібних баз даних надають численні системи типу Cronos (оболонки, поширювані цілком легально). За допомогою подібних інструментальних засобів будь-якому зацікавленому користувачу мережі Інтернет стають доступні численні бази даних, які працюють під цими оболонками.

Авторське право. Можна виділити три класи основних проблем авторського права, що мають відношення до конкурентної розвідки. Це проблеми, пов’язані з такими факторами:

- правомірністю використання вхідної інформації (джерел інформації), на підставі якої формуються звіти – результати конкурентної розвідки;
- проблем з авторськими правами на результати конкурентної розвідки;
- правами на застосування (використання) спеціалізованого програмного забезпечення, необхідного для проведення конкурентної розвідки.

Крім того, одна з проблем, що стоїть перед службами конкурентної розвідки в Україні – практично повна відсутність антидемпінгового законодавства.

Ситуація може змінитися, якщо буде створена чітка правова база для конкурентної розвідки.

Авторське право є однією з форм захисту, опублікованих і неопублікованих робіт, передбачених главою 17 Кодексу США, що визначає авторів "оригінальних робіт авторів", в тому числі літературних, драматичних, музичних і художніх творів. Національні закони про авторські права є обмеженнями конкурентної розвідки. Незважаючи на це, все ж залишаються можливості правомірного використання конкурентної розвідки, що визначається чотирма факторами:

- метою і характером використання;
- властивостями, які використовуються авторських робіт;
- кількістю і частинами авторської роботи, які використовуються;
- впливом використання авторських робіт на потенційний ринок або цінність цих робіт.

Конкурентна розвідка і захист комерційної таємниці. Важливе значення для становлення конкурентної розвідки мав ряд статей Закону України "Про захист від недобросовісної конкуренції" від 07.06.96 р. № 236/96-ВР [21], де (ст. 15-1), забороняється "Неправомірне збирання комерційної інформації", "Розголошення комерційної інформації ", "Неправомірне використання комерційної інформації" (гл. 4, ст. 16, 17, 19, відповідно).

На цей час українське законодавство про охорону службової та комерційної таємниці являє собою сукупність статей, які містяться в різних правових актах, присвячених в цілому регулюванню інших суспільних відносин.

Поняття комерційної таємниці дано в ст. 505 п. 1 Цивільного кодексу України. Комерційна інформація підлягає захисту, а її втрата може призвести до значних негативних наслідків. Комерційну таємницю яка містить певні рішення, способи, креслення, які часто не можна захистити шляхом отримання охоронних документів, або отримання таких охоронних документів фактично призведе до розкриття інформації, тому таку інформацію суб'єкт господарювання змушений зберігати та охороняти всіма доступними способами. Цивільний кодекс України, визначає комерційну таємницю (ст. 505 п. 1) як інформацію, "яка є секретною в тому розумінні, що вона в загальному або в певній формі та сукупності є невідомою та не легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів стосовно збереження її секретності, вжитих особою, яка законно контролює цю інформацію".

Відповідно до цих визначень, як тільки інформація в результаті будь-яких дій потрапляє, наприклад, на сторінки веб-сайту, вона перестає вважатися комерційною таємницею, тому що стає легкодоступною.

Комерційна таємниця віднесена ст. 420 Цивільного кодексу України до об'єктів права інтелектуальної власності.

Хоча в багатьох статтях Кримінального кодексу України (ст. 231, 232, 232-1, 361, 363) встановлено кримінальну відповідальність як за розголошення комерційної таємниці, так і за незаконний збір і використання відомостей, що до неї відносяться, однак, існуюча нормативно-правова база чітко не регламентує, які саме відомості щодо фінансово-господарської діяльності підприємства є комерційною таємницею (за винятком хіба що банківської таємниці, визначення якої дано в ст. 60 Закону України "Про банки і банківську діяльність" [22]).

У Постанові Кабінету Міністрів України "Про перелік відомостей, які не становлять комерційної таємниці" від 09.08.93 р. № 611 визначено цілий клас документів, що стосуються діяльності бізнес-структур, які є фактично відкритими,

зокрема, установчі документи, форми звітності, інформація про участь засновників і посадових осіб в інших компаніях і т.п.

Найчастіше зусилля конкурентної розвідки спрямовані на отримання комерційної таємниці конкурентів. І хоча в різних законодавчих актах даються різні формулювання, можна погодитися з тим [23], що комерційні таємниці характеризується такою сукупністю ознак: інформація є секретною, є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якої вона відноситься; в зв'язку з тим, що є секретною, вона має комерційну цінність. Таким чином, комерційна таємниця – це інформація, яка є корисною і не є загальновідомою. Вона має дійсну або комерційну цінність, з якої можна мати прибуток і для захисту якої власник вживає заходів у всіх сферах життя і діяльності. Таким чином, можна сказати, що діяльність бізнес-розвідки іноді спрямована на видобуток інформації, яка не є загальнодоступною і охороняється законом. Ці діяння порушують величезну кількість статей Кримінального Кодексу України, зокрема, статтю 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю".

Таким чином, бізнес-розвідка може легітимно використовувати лише ті методи і способи збору і обробки інформації, що не суперечать законодавству, тобто основні функції конкурентної розвідки – якісний збір, систематизація і, головне, аналіз інформації, а не стеження, підкупи і незаконні хакерські зломи.

Вперше у нас право на збереження комерційної таємниці було проголошено Законом СРСР "Про підприємства в СРСР" від 4 червня 1990 року. У ст. 33 зазначеного Закону розкривалося поняття комерційної таємниці як "відомостей, що не є державними секретами, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємств, розголошення (передача, витік) яких може завдати шкоди їх інтересам".

Конкурентна розвідка і захист персональних даних. Приватність, разом з правом на захист життя та свободою слова, є фундаментальними цінностями людства.

Персональні дані, тобто інформація про людей, все більше перетворюється в найдорожчий товар. Така інформація в руках зловмисника – потужна зброя. Державні установи, банки, великі корпорації не завжди можуть забезпечити захист баз персональних даних, які зберігаються у них, в результаті чого, величезний потік конфіденційної інформації надходить на ринок. Тобто персональні дані необхідно захищати.

На сьогодні, основними європейськими правовими стандартами в галузі захисту персональних даних є Конвенція Ради Європи "Про захист осіб у зв'язку з автоматичною обробкою персональних даних" від 28 січня 1981 року (ETS № 108) та "Пакет захисту даних" Європейського Парламенту та Ради від 27 червня 2016 року [24], які є обов'язковими для всіх держав-членів Європейського Союзу і які є предметом для наслідування в області законодавства, в тому числі, і нашою країною. Країни Євросоюзу мають приводити своє законодавство у відповідність зазначеним правовим стандартам.

Ще в 1998 році у Великобританії був прийнятий "Закон про захист персональних даних" – "Data Protection Act 1998". Його технічна реалізація – проект стандарту "Specification for the management of personal information in compliance with the Data Protection Act 1998" (BS 10012, 2009).

Паралельно з цим свою версію стандарту з безпеки персональних даних випустили в США. Проект документа щодо захисту персональних даних для американських державних структур – "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (SP 800122) регламентує виконання Законів "The Privacy Act of 1974" і "Privacy Protection Act of 1980".

Канада випустила “Privacy Code” – набір документів для реалізації законодавства щодо захисту відомостей щодо приватних осіб (The Privacy Act і PIPEDA).

У державах-членах Євросоюзу визначення персональних даних, як правило, максимально широкі, в результаті чого громадянами на практиці часто не виконується відповідне законодавство через його зайве “навантаження”. Відповідні органи державної влади, як правило, не роблять ніяких дій, окрім особливих випадків. Важливими залишаються питання виникнення колізій між вимогами приватності та інтересами свободи слова. Сучасними європейськими законами, як правило, забороняється збирання, зберігання, використання та поширення без згоди суб’єкта даних саме критичних персональних даних.

Право на приватність гарантується Конституцією України. Стаття 32 Конституції України говорить: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України”. Крім того в Конституції України передбачений захист ще деяких аспектів приватності. Так, стаття 30 захищає недоторканність житла (територіальна приватність), стаття 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційна приватність), стаття 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а стаття 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи іншим дослідженням (захищаючи елементи фізичної приватності).

Конвенція РЄ про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ратифікована Україною 06.07.2010 р.) визначає положення стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки.

Наступні дані, що часто використовуються для вирізнення конкретної особи, означені як особові Управлінням США з менеджменту й бюджету:

- повне ім’я, якщо не поширені (мається на увазі ім’я разом із прізвищем);
- національний ідентифікаційний номер;
- IP-адреса (у деяких випадках);
- номерний знак транспортного засобу;
- номер водійських прав;
- обличчя, відбитки пальців, або почерк;
- номери кредитних карток;
- цифрова ідентичність (цифровий підпис);
- дата народження;
- місце народження;
- генетична інформація.

Згідно із законодавством більшості європейських держав особові дані розділяються за критерієм “чутливості” на дані загального характеру і “чутливі” (вразливі) особові дані.

Загальні особові дані:

- ідентифікаційні дані (прізвище, ім’я, по батькові, адреса, телефон тощо);
- паспортні дані;
- особисті відомості (вік, стать, сімейний стан тощо);
- склад сім’ї;
- освіта;
- професія;

- житлові умови;
- спосіб життя;
- життєві інтереси та захоплення;
- споживчі звички;
- фінансова інформація.

“Чутливі” особові дані:

- інформація про расове, етнічне походження та національність;
- відомості, що стосуються політичних, світоглядних та релігійних переконань;
- відомості про членство в політичних партіях, профспілках, релігійних або громадських організаціях;
- відомості про стан здоров’я і статеве життя;
- генетичні і біометричні дані;
- місце знаходження та шляхи пересування особи;
- інформація щодо застосування до особи заходів в рамках трудового слідства;
- інформація щодо вчинення щодо особи різних видів насильства.

Для з’ясування, яке ж відношення має фізична особа або компанія до захисту персональних даних, велике значення має визначення суб’єктів відносин, пов’язаних із персональними даними (стаття 4 Закону України “Про захист персональних даних” від 01.06.10 р. № 2297-VI): “Суб’єктами відносин, яка пов’язана з персональними даними, є:

- суб’єкт персональних даних;
- власник бази персональних даних;
- розпорядник бази персональних даних;
- третя особа;
- уповноважений державний орган з питань захисту персональних даних;
- інші органи державної влади і органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних”.

В українському законодавстві передбачено повідомний характер обробки персональних даних. Власник або розпорядник (оператор) до початку обробки персональних даних зобов’язаний повідомити уповноважений орган із захисту прав суб’єктів персональних даних про свій намір здійснювати обробку персональних даних. Потім дані про власників або розпорядників (операторів) вносяться до спеціального реєстру операторів. Інформація, що міститься в реєстрі операторів, стає загальнодоступною.

Закони про персональні дані стосуються більшості населення як учасників процесу “обробки” даних. А так як суб’єктом персональних даних є кожна людина, то Закон має загальний характер і стосується кожного. Зокрема, персональні дані широко використовуються в соціальних мережах і сервісах електронної пошти.

Сучасна Інтернет-компанія збирає і обробляє різні категорії персональних даних – своїх співробітників, своїх контрагентів за договорами і деякі дані користувачів своїх сервісів. Люди, що розміщують інформацію про себе в соціальних мережах або службах знайомств, свідомо роблять її відкритою для всіх користувачів ресурсу, і по закону її можна трактувати як “загальнодоступну”, а значить, дотримання особливого режиму конфіденційності щодо її не потрібно, але в соціальних мережах є і інформація, яку користувач приховує, роблячи її доступною тільки для окремої групи користувачів (“друзів”). У цьому випадку Інтернет-ресурс повинен передбачати для неї спеціальні засоби захисту.

Підрозділи конкурентної розвідки займаються обробкою персональних даних, які знаходяться у відкритих джерелах в мережі Інтернет, тобто є загальнодоступними. Для

їх обробки згоди суб'єкта персональних даних не потрібно. Однак при цьому обов'язок доведення, що оброблювані персональні дані є загальнодоступними, покладається на власника або розпорядника. А це означає, що необхідно або накопичувати докази того, що дані взяті з загальнодоступних джерел, або отримувати згоду від суб'єкта персональних даних і потім зберігати цей документ. Крім того, потрібно мати документ, що підтверджує загальнодоступність джерела персональних даних. При цьому залишається без відповіді питання доведеності того, що власник інформаційного ресурсу (веб-сайту) володіє письмовою згодою на обробку.

Правові питання керування репутацією. Одне з важливих завдань конкурентної розвідки – керування репутацією, оцінювання, отримання інформації щодо репутації об'єкту розвідки. Репутація представляє собою соціальну оцінку групи суб'єктів про людину, групу людей або компанії, що сформувалася на основі деяких критеріїв. Репутація компанії – це комплекс оціночних уявлень цільової аудиторії про компанію, сформований на основі факторів репутації, які мають значення для цієї аудиторії. Відповідно до інформаційного листа Вищого господарського суду України "Про деякі питання практики застосування господарськими судами законодавства про інформацію" від 28.03.07 р. ділову репутацію юридичної особи становить престиж її фірмового (комерційного) найменування, торговельних марок та інших належних їй нематеріальних активів серед кола споживачів її товарів та послуг.

Успіх компанії безпосередньо пов'язаний з її репутацією. Так дослідження, проведене австралійськими вченими П. Робертсом і Г. Даулінгом [25], виявило, що чим вище репутація у компанії, тим, по-перше, довше період, протягом якого вона отримує максимальний дохід від своєї діяльності, і, по-друге, тим менше часу компанії потрібно для досягнення середніх по галузі фінансових показників при впровадженні інновацій. Грошовий же еквівалент ділової репутації може бути виражений у формі гудвілу (goodwill). Відповідно до Міжнародних стандартів фінансової звітності (МСФЗ) гудвіл, являє собою різницю між ціною, заплаченою за підприємство покупцями, і "справедливої вартості" (дана величина часто значно відрізняється від простої вартості всіх активів фірми). Наприклад, в правилах бухгалтерського обліку під репутацією розуміється "різниця між купівельною ціною організації та вартістю по балансу всіх її активів і зобов'язань".

Щоб мати можливість з'ясовувати нематеріальну ціну компанії, розробляються експертні оцінки репутації. Вартість репутації може визначатися експертами, наприклад, таким чином. Спочатку розраховується дохід, отриманий компанією за рахунок бренду, а потім отримана сума множиться на спеціально розрахований коефіцієнт (залежить від положення компанії в галузі, стабільності фінансових показників і т. і.).

Існують і непрямі оцінки рівня репутації компаній, наприклад, засновані на результатах опитування керівників фірм і аналітиків, які оцінюють компанії за такими параметрами, як якість менеджменту і продукту, здатність залучити й утримати кваліфіковані кадри, фінансова стабільність, ефективне використання активів, інвестиційна привабливість, застосування нових технологій і т.п.

Поняття "керування репутацією в Інтернеті" (Online Reputation Management, ORM) по суті являє собою комплекс заходів з виявлення в мережі негативного контенту і зведення його до мінімуму в соціальних медіа і в результатах пошукової видачі. Це, свого роду, PR-кампанія в кіберпросторі. Гілкою ORM є SERM (Search Engine Reputation Management) – пошукове керування репутацією. Зростання ORM в рік у світі в останні роки становить близько 30 %.

Роботи з керування репутацією проводять як спеціалізовані PR-агентства, що працюють на теренах веб-простору, так і підрозділи SEO-агентств, які запускають PR-кампанії, спрямовані на пошук і усунення негативного контенту, співпрацюючи із службами конкурентної розвідки. Основне завдання керування репутацією – формування позитивного іміджу про компанії та її продукти. Зазвичай зусилля концентруються в трьох областях: пошуковій видачі, відгуках в електронних ЗМІ та згадках в соціальних медіа.

Керування репутацією в пошукових системах (Search Engine Reputation Management, SERM) – комплекс заходів, спрямованих на виключення негативних відгуків про компанію, товар або послугу в результатах видачі пошукової системи.

Негативна інформація, що завдає шкоди репутації в мережі, може бути різного походження. Умовно виділяють основні групи походження негативного контенту:

- ненавмисний негатив. Зазвичай такий негатив не представляє великої загрози, але ігнорувати його ні в якому разі не можна;
- умисний негатив з метою вдарити по репутації, наприклад, негативні відгуки звільнених співробітників;
- чорна PR-кампанія – найнебезпечніший вид негативного контенту, що завдає серйозного удару по репутації. Такі PR-кампанії проводять фахівці, які ретельно вивчають бізнес конкурента і точно знають, де прихована ахіллесова п’ята.

Найбільш уразливими тематиками в плані тяжіння негативних відгуків можна назвати:

- банки, фінансові інститути;
- діячі політики і шоу-бізнесу;
- туризм, подорожі (відгуки);
- мобільна техніка і зв’язок;
- побутова техніка;
- заклади громадського харчування.

Відповідно, розміщується і розповсюджується негативний контент на різних майданчиках:

- блоги і форуми;
- соціальні мережі;
- тематичні веб-сайти і портали;
- спеціалізовані сервіси відгуків.

Боротися з негативним контентом покликане пошукове керування репутацією – SERM. Завдання SERM складається у витісненні з результатів пошуку веб-сторінок з небажаною інформацією, в результаті чого цільова аудиторія перестане бачити такі ресурси, так як користувачі не будуть виходити на них за допомогою пошукових систем. Для досягнення цієї мети створюються матеріали з позитивним контентом, припускаючи, що вони витіснять негативні небажані повідомлення. Для розміщення позитивного контенту (з метою витіснення негативного) використовуються найавторитетніші веб-ресурси:

- великі новинні ресурси;
- тематичні портали;
- галузеві форуми;
- персональні блоги та особисті сайти споживачів.

Як простір моніторингу для керування репутацією вибирають мережеві ресурси, де розміщуються відгуки споживачів:

- соціальні мережі, месенджери;

- блоги і форуми;
- тематичні веб-сайти і портали;
- спеціальні сервіси відгуків.

Одним з критеріїв якості послуги моніторингу репутації є повнота охоплення – частка інформації про об'єкт, що досліджується під час роботи від загального обсягу інформації в мережі про об'єкт. Як і раніше основним інструментом пошуку інформації є традиційні пошукові системи, вони охоплюють значну частину Інтернет-контенту, а також деяку частину соціальних медіа.

Висновки.

У роботі було розглянуто поняття конкурентної розвідки, сфер її застосування, правових обмежень і можливостей її застосування. Розглянуті легітимні джерела інформації, а також основні проблемні моменти, пов'язані з питаннями захисту комерційної таємниці, персональних даних, авторських прав та суміжних питань. Розглянуто роль конкурентної розвідки в управлінні репутацією в мережах.

Показано, що актуальність конкурентної розвідки останнім часом значно зросла в усьому світі. Це пов'язано з такими процесами, як глобалізація економіки, зростання конкуренції, цифровізації, віртуалізація економіки, розвиток інформаційних технологій.

Враховуючи тенденції розвитку суспільства і інформаційних технологій, застосування та подальший розвиток правових аспектів конкурентної розвідки може стати основою створення дієвих інструментів формування сучасного бізнес-середовища.

Використана література

1. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. Київ: ИПРИ НАН Украины, 2013. 248 с.

2. Дудихин В.В., Дудихина О.В. Конкурентная разведка в Интернет. Москва: АСТ, НТ Пресс, 2004. 240 с.

3. Ландэ Д., Прищепа В. Школа веб-разведки. Инструменты и источники. *Телеком.* 2007. № 7–8. С. 46-49.

4. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, 2019. № 1. P. 103-108. OSINT Academy. URL: https://www.youtube.com/playlist?list=PL-9OTQQwXf2XuDGO_EIewUOpzUXLDDfcL

5. Берд К. Модель OSINT. *Компьютерра.* 2007. № 22.

6. Army techniques publication FMI 2-22.9. Headquarters Department of the Army Washington, DC, 7 2012.

7. Steele, R.D. Open Source Intelligence: READER Proceedings, 1997 Volume II 6th International Conference & Exhibit Global Security & Global Comp, 1997. P. 329-341.

8. Кондратьев А. На основе открытых источников. *ВПК.* 2009. № 36 (302).

9. Paulson, T.M. Intelligence Issues & Developm. Nova Publishers, 2008.

10. Ланде Д.В. Побудова моделей предметних областей з юриспруденції за даними сервісу Wikipedia. *Інформація і право.* № 4(19)/2016. С. 39-46.

11. Lande D.V., Andrushchenko V.B., Balagura I.V. Formation of the Subject Area on the Base of Wikipedia Service.: материалы междунар. науч.-техн. конф. *Open Semantic Technologies for Intelligent Systems,* г. Минск, 16 – 18 февраля 2017 г. Минск: БГУИР, 2017. Вып. 1. С. 211-214.

12. Нежданов И. Технологии разведки для бизнеса. Москва: Ось-89, 2009. 400 с.

13. Про інформацію: Закон України від 02.10.92 р. № 2657-XII.

14. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII.

15. Про охоронну діяльність: Закон України від 22.03.12 р. № 4616-VI.

16. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI.

17. Питання європейської та євроатлантичної інтеграції: Указ Президента України від 20.04.19 р. № 155/2019.

18. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16 р. № 242/2016.

19. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII.

20. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016.

21. Про захист від недобросовісної конкуренції: Закон України від 07.06.96 р. № 236/96-ВР.

22. Про банки і банківську діяльність: Закон України від 07.12.00 р. № 2121-III.

23. Основи методики розслідування незаконного збирання та розголошення комерційної таємниці. *Юридичний журнал.* 2006. № 8. С. 48-66.

24. Пилипчук В.Г., Брижко В.М. та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с. С. 37-45.

25. Roberts, P.W., Dowling, G.R. Corporate reputation and sustained superior financial performance. *Strategic Management Journal.* 2002. № 12. P. 1077-1093.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~