УДК 334.7:004:34

М. О. Живко

Правові аспекти захисту інформації суб'єктів господарювання

Розглянуто основні аспекти захисту інформації суб'єктів господарювання, особливо в умовах масової комп'ютеризації. Визначено роль структурних підрозділів конкурентної розвідки та їх відмінність від промислового шпигунства, правові аспекти взаємодії зі службами безпеки щодо захисту конфіденційної інформації.
Ключові слова: нормативно-правове регулювання, інформаційне забезпечення, інформаційні технології, комп'ютерні системи (КС), захист інформації, конкурентна розвідка, промислове шпигунство.

[1] В умовах інтеграції та гострої конкурентної боротьби проблема пріоритетів використання науково-технічних досягнень стає першочерговою. Для задоволення потреб сучасного суспільства виникає проблема інформаційного забезпечення всіх сфер діяльності людини, і як одна із найважливіших – надійний захист інформації. Особливої гостроти ця проблема набуває у зв'язку з масовою комп'ютеризацією, об'єднанням електронної техніки у комп'ютерні мережі та використання Інтернет.

З розвитком сучасних інформаційних технологій в управлінні, економіці, банківській сфері набули поширення злочини у сфері нових інформаційних технологій. Основою скоєння злочинів є витоки конфіденційної інформації суб'єктів господарювання, яка визнається комерційною таємницею. Ці злочини характеризуються неможливістю фіксації та наочного спостереження, труднощами з'ясування місця скоєння злочину, широким спектром засобів кодування інформації, недостатніми зв'язками між окремими епізодами у самій сукупності доказів та швидкодії знищення даних доказів.

Вибір серед сукупності сучасних методів і засобів захисту тих, які будуть найбільш відповідати певним вимогам щодо сфери застосування

та забезпечення достатнього рівня безпеки суб'єкта господарювання, є складним завданням. Водночас різні технології захисту мають багато спільних рис із огляду як розробки, так і використання. Це дає можливість вивчати сучасні технології на прикладах, які, незважаючи на новизну, вже стали класичними.

Забезпечення інформаційної безпеки завжди було одним із найважливіших напрямків діяльності держави, сьогодні воно гостро стоїть на рівні служб безпеки суб'єктів господарювання. Серед вітчизняних науковців, які досліджують на достатньо серйозній методологічній основі проблеми національної безпеки взагалі, та її складової інформаційної безпеки зокрема, можна назвати таких як: В. Горбулін, Н. Нижник, Г. Ситник, В. Білоус, О. Данільян, О. Дзьобань, М. Панов, В. Ліпкан, М. Левицька, О. Бодрук, О. Гончаренко, Є. Лісіцин, Ю. Максименко, В. Желіховський, Б. Кормич, О. Юдін, В. Богуш та інші.

Питаннями дослідження проблем, пов'язаних із розслідуванням злочинів у сфері інформаційних технологій займались такі учені як Б. В. Вехов, В. О. Голубєв, О. Ф. Долженков, В. В. Крилов, В. Я. Мацюк, В. А. Некрасов, М. В. Салтевський, І. В. Сервецький, І. Ф. Хараберюш та інші [2, 4].

Не зважаючи на чималу кількість різних наукових праць та досліджень питання правового регулювання, стратегії та організаційно-тактичні основи діяльності служб конкурентної розвідки, інформаційно-аналітичних та маркетингових служб компаній, використання технічних засобів для захисту інформації і протидії злочинності у сфері інформаційних технологій потребують подальших наукових досліджень.

Мета статті полягає у розкритті інформаційної безпеки та конкурентної розвідки компанії як складових частин служби безпеки компанії, вагомих факторів захищеності її комерційних інтересів як в інформаційній сфері, так і в економіці загалом, що визначаються сукупністю збалансованих інтересів особистості, суб'єкта господарювання та суспільства.

Інструментами розв'язання проблем інформаційної безпеки стають конкурентна розвідка та промислове шпигунство, тобто, дві сторони однієї проблеми: позитивна та негативна. Особливо вітчизняні суб'єкти господарювання реально відчувають на собі вплив інтеграційних процесів в Україні, адже їм відкриваються переваги і недоліки сучасних новітніх процесів світового господарювання, механізації та автоматизації виробничих процесів, нові ризики, нові сподівання. Найпоширенішими серед них є факти протиправного і шпигунського вивідування, викрадення та несанкціонованого зняття комерційно важливої для компанії інформації. Розглянемо правові механізми захисту конфіденційної інформації суб'єкта господарювання.

Поняття «розвідка» розглядається як процес отримання якихось відомостей, що є важливими та вагомими для певного кола споживачів. В наукових та публіцистичних джерелах ми часто зустрічаємо поняття «економічна розвідка», «ділова розвідка», «корпоративна розвідка», «бізнес-розвідка», «конкурентна розвідка» тощо. Зокрема, дослідження загальнодоступних джерел інформації, що відображають основні тенденції бізнесу й наміри конкурентів, аналізу ризиків, дають можливість стверджувати, що на Заході професійно закріпилось поняття «конкурентна розвідка» *(competitive intelligence)*. У національному інформаційному просторі найбільш вживаними є поняття «ділова розвідка» та «бізнес-розвідка», які здебільшого замінюють термінами «інформаційно-аналітична робота», «моніторинг» тощо [2, 3].

Для розкриття суті проблеми визначимо спорідненість та відмінність між поняттями «конкурентна розвідка» і «промислове шпигунство». Спільною рисою обидвох понять є процес отримання інформації, а відмінною – методи отримання інформації, власне види інформації, яку намагаються отримувати суб'єкти господарювання та правовий статус «конкурентної розвідки» і «промислового шпигунства».

Конкурентна розвідка – це постійний процес збору, нагромадження, групування, аналізу інформації про внутрішнє і зовнішнє середовище компанії та передачі її керівництву для прийняття управлінських рішень з метою запобігання та управління ризиками, підвищення

конкурентноздатності продукції, ефективності виробництва та отримання прибутків. Конкурентна розвідка займається збором інформації про навколишнє бізнес-середовище лише законними способами і методами. Тобто, конкурентна розвідка – це складова корпоративної культури сучасного бізнесу. Поділ вхідної інформації суб'єктів господарювання на види зображено на рисунку 1.

Пошук інформації в Україні не заборонений законом, тобто збирати інформацію може кожен суб'єкт господарювання чи громадянин зо-

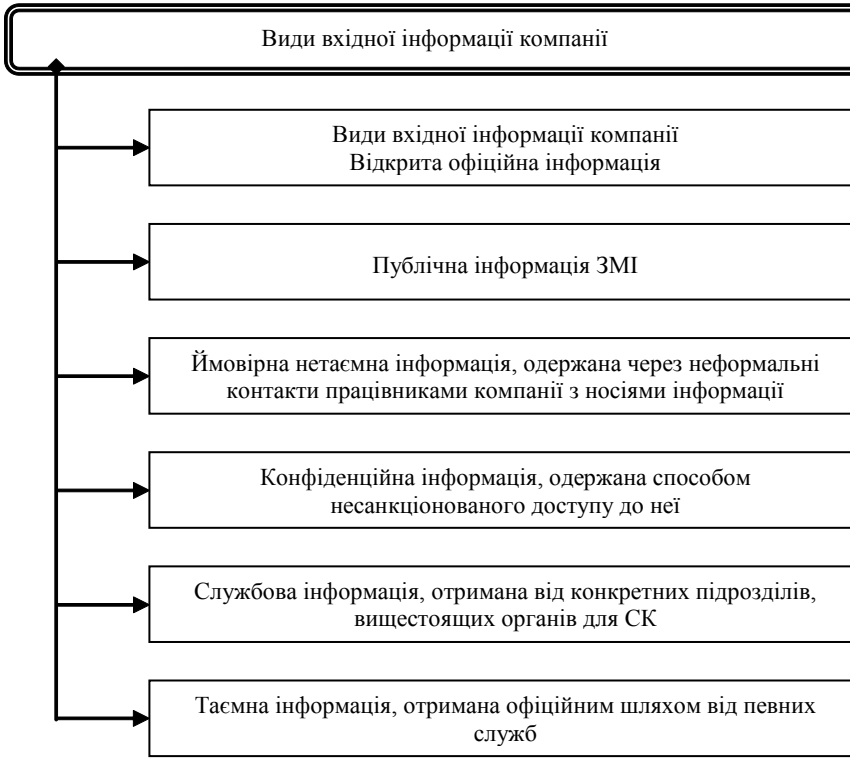

Рис. 1. Поділ вхідної інформації суб'єктів господарювання на види

крема при умові – не використовувати заборонених методів, що порушують гарантовані Конституцією права і свобода людини. Про бізнес-структури можна дізнатися 90-95% правдивої та корисної інформації з цілком легальних джерел: з Інтернету, з друкованих засобів масової інформації, під час проведення професійних семінарів, конференцій, виставок [7].

Конфіденційною інформацією є будь-яка інформація, яка безпосередньо може не стосуватися господарської діяльності компанії, однак впливати на її фінансово-господарський процес та на правовідносини з третіми особами.

Конкурентна розвідка діє виключно в рамках існуючих законів. Поява нових інформаційних технологій (Internet, професійних баз даних, систем пошуку інформації) і відносна дешевизна доступу до інформаційних ресурсів дозволяють аналітикам готувати якісні матеріали, придатні для ухвалення рішень керівництвом компаній. При цьому вони працюють тільки з відкритими джерелами інформації. Аналогічні технології обробки відкритої інформації використовують всі спецслужби світу. Але для КР найважливішою умовою є дотримання етичних норм і принципів діяльності виключно в рамках чинного законодавства [5].

Конкурентна розвідка на відміну від промислового шпигунства проводиться в межах правового поля та етичних норм.

Промислове шпигунство стосовно бізнесу є різновидом економічного шпигунства, способом конкурентної боротьби, який використовує будь-які неетичні методи ведення розвідки. Промислове шпигунство здійснюється протиправними методами і спрямоване на отримання незаконним шляхом конфіденційної інформації, що становить комерційну таємницю компанії.

Згідно з чинним законодавством, шпигунство є злочином і карається кримінальним законом, а значить і промислове шпигунство за справедливим твердженням А. Марущака є діянням, що підпадає під ознаки складів злочинів, передбачених статтями 231 Кримінального кодексу України «Незаконне збирання з метою використання або використання

відомостей, що становлять комерційну або банківську таємницю» і 232 Кримінального кодексу України «Розголошення комерційної або банківської таємниці». Тобто промислове шпигунство – це злочинна діяльність, яка посягає на охоронювані законодавством інтереси [7]. Таким чином все, що використовується розвідником, є законним. Промислове шпигунство, навпаки, передбачає нелегальні методи і технології. Для встановлення межі правомірної поведінки пошукувачів конкурентно-важливої інформації варто визначитись із суб'єктивними та об'єктивними ознаками статей 231 і 232 Кримінального кодексу України [10].

Сучасний стан і прогресування злочинності підтверджує її перетворення у специфічну антигромадську систему, яка характеризується у державних концепціях як загроза національній безпеці України. На розв'язання цієї проблеми спрямовані процеси структурного реформування правоохоронних органів, розробка нових форм та методів оперативно-розшукової діяльності, використання сучасних основ оперативно-технічних засобів для протидії та розкриття злочинів у сфері нових інформаційних технологій, запровадження світового досвіду для такої протидії. Термін «протидія» в етимологічному значенні – це дія, яка спрямована проти іншої дії, перешкоджає їй [1, с. 992].

Інформаційна безпека – захищеність інформації, що має циркулювати в інтегрованих інформаційних автоматизованих системах (ІІАС), та підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, здатних завдати збитків власникам або користувачам інформації та підтримуючій інфраструктурі. Наше визначення, що інформаційна безпека – стан правових і відповідних інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [8, с. 67].

Доводиться констатувати, що незважаючи на актуальність інформаційної складової національної безпеки України, на сьогодні у вітчизняному законодавстві відсутня норма, яка б містила чітку дефініцію поняття «інформаційна безпека», враховуючи різницю між

інформаційною безпекою та безпекою інформації. Для всебічного розгляду поняття «інформаційна безпека» та, використовуючи запропонований В. Ліпканом алгоритм дослідження базового поняття, зупинимося детальніше на кожній з груп.

Так, Закон України «Про основи національної безпеки України» від 19 червня 2003 р. та інші нормативно-правові акти, спрямовані на регулювання суспільних відносин в інформаційній сфері, практично нормативно не закріплюють вищезазначених понять [10, 11].

Дана теза підтверджується нормами єдиного нормативно-правового акту, в якому здійснено спробу щодо окреслення загальних підходів до розуміння сутності даного феномена – Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року [10].

Згідно з цим документом інформаційна безпека виступає невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки вважаються інформаційні ресурси, канали інформаційного обміну та телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Результатом виконання Програми мав би стати пакет нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високотехнологічні та надійні криптографічні методи захисту інформації тощо [9].

Сьогодні в Україні існує близько трьох тисяч нормативно-правових актів, які регулюють, захищають та підтримують суспільні відносини щодо інформації. Основу законодавства України про інформацію й інформатизацію складають: Конституція України, ціла низка Кодексів, Закон про інформацію, Закон про захист інформації в автоматизованих системах і ряд інших спеціальних Законів.

Закони та підзаконні нормативно-правові акти, як і все право, виконують регуляторну, охоронну, дозвільну, заборонну, захисну функцію. Однак, нормативні положення щодо охорони та захисту конфіденційної інформації суб'єктів господарювання, інформації в комп'ютеризованих інформаційних системах, які розроблені раніше, не відповідають рівню розвитку суспільства стосовно сучасних інформаційних технологій. Це пояснюється тим, що дані документи приймалися в різний час, їх проекти розроблялися різними групами науковців, які не взаємодіяли між собою та приймали положення, що часом мали суперечливий характер. Недостатній рівень державної підтримки цих розробок призвів до того, що вказані проекти відстають від потреб захисту інформації та мають фрагментарну, організаційно-роз'єднану та, часом, суперечну суть.

Зважаючи на це, використання комп'ютерних систем в умовах сучасного бізнесу для захисту інформації залежить від двох головних функцій правового забезпечення: регуляторної, що передбачає встановлення правового режиму розроблення, створення, функціонування і взаємодії служб конкурентної розвідки та інформаційної безпеки, їхнього правового статусу; захисної, що обумовлює встановлення чіткого регламенту доступу обслуговуючого та технічного персоналу до інформації та комп'ютерних систем; розмежуванні доступу до службової інформації; в юридичній відповідальності власників і персоналу інформаційних систем за порушення цілісності інформації та юридичній відповідальності, за порушення прав власності на інформацію.

Список використаних джерел

1. Великий тлумачний словник сучасної української мови / Уклад. і гол. ред. В.Т. Бусел. – Ірпінь : Перун, 2001. – 1440 с.
2. Живко М. О. Захист інформації в системі економічної безпеки держави та підприємства : матеріали III українсько-польської НПК. / М. О. Живко // Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія. – Львів, 2006. – С. 270-277.

3. Живко М. О. Інформаційна безпека України через призму національної безпеки : зб. тез міжнародної науково-практичної конференції (22-23 березня 2007 року) // Психологічні аспекти національної безпеки) / М. О. Живко – Львів: Арал, 2007. – С. 86 – 87.
4. Живко З. Б. Особливості кадрового забезпечення служби конкурентної розвідки в економічній безпеці фірми / З. Б.Живко, М. О. Живко, О. Й. Хомин // Науковий вісник ЛДУВС. – Львів, 2006. – Вип. 2. – С. 306–327. – (Серія економічна).
5. Живко З.Б., Живко М.О. Регламентація конкурентної розвідки в інформаційно-правовому просторі : Зб. наук. праць / З. Б. Живко, М. О. Живко // Науковий вісник ЛДУВС. – 2007. – Вип. 2. – С. 211-219. – (Серія юридична).
6. Інформатизація, право, управління (організаційно-правові питання) : монографія / Р. А. Калюжний, О. Д. Крупчан, В. Д. Гавловський, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець / за заг. ред. М. Я. Швеця, О. Д. Крупчана. – К. : НДЦ правової інформатики АПрНУ, 2002. – 191 с.
7. Марущак А. Протидія злочинним та конкурентним механізмам доступу до інформації про суб'єкта господарювання / А. Марущак. – Сайт юридичного журналу «ЮСТІНІАН» http://www.justinian.com.ua.
8. Спеціалізований словник економічних термінів: банківська справа, контроль і ревізія, судова бухгалтерія, реклама, менеджмент, захист інформації, економічна безпека, маркетинг / З. Б. Живко, М. О. Живко. – Львів : УАД, 2006. – 150 с.
9. Цимбалюк В. С. Правова база інформаційної безпеки // Веб-сайт : http://www.security.ukrnet.net/.
10. Сайт Верховної Ради України // Веб-сайт : http://www.rada.kiev.ua.
11. Сайт ЛІГА: Закон // Веб-сайт : www.ligazakon.ua; CD-версія системи.

Живко М. А. **Правовые аспекты защиты информации субъектов ведения хазяйства.**

Рассмотрены основные аспекты защиты информации субъектов ведения хозяйства, в частности в условиях массовой компьютеризации. Определена роль структурных подразделений конкурентной разведки и их отличие от промышленного шпионажа, правовые аспекты взаимодействия со службами безопасности относительно защиты конфиденциальной информации.

Ключевые слова: нормативно-правовое регуляция, информационное обеспечение, информационные технологии, компьютерные системы (КС), защита информации, конкурентная разведка, промышленный шпионаж.

Zhivko M. A. **Legal Aspects of Priv Subjects of Menage.**

The basic aspects of defence of information of subjects of menage are considered, in particular in the conditions of mass computerization. The role of structural subdivisions of competition secret service and their difference is certain from industrial espionage, legal aspects of co-operating with services of safety in relation to defence of confidential information.

Key words: normative-legal adjusting, informative providing, information technologies, computer systems (KS), defence of information, competition secret service, industrial espionage.

УДК 347. 451. 2

І. В. Апопій

Договір поставки в цивільному та господарському законодавстві: проблеми та шляхи їх подолання

Досліджено ступінь досконалості правового регулювання договору поставки в ринковому середовищі, проаналізовані основні розбіжності та суперечності між Цивільним та Господарським кодексами у даній сфері, сформульовано низку пропозицій щодо вдосконалення чинного законодавства, зокрема внесення змін та доповнень у згадані кодекси з метою оптимізації правового забезпечення договору поставки.

Ключові слова: договір поставки, господарський кодекс, цивільний кодекс.

Розвиток національної економіки з «нахилом» у комерційну діяльність, розширення масштабів обігу товарів, зростання кількості