Цивільне право і цивільний процес

УДК 347.77

Новицький Владислав Миколайович
аспірант кафедри
права інтелектуальної власності та корпоративного права
Національного університету «Одеська юридична академія»
Новицкий Владислав Николаевич
аспирант кафедры
права интеллектуальной собственности и корпоративного права
Национального университета «Одесская юридическая академия»
Novitsky Vladislav
Graduate Student of the Department of
Intellectual Property Law and Corporate Law of the
National University "Odessa Law Academy"

ОСНОВНІ ЗАГРОЗИ ВТРАТИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В МЕРЕЖІ ІНТЕРНЕТ ТА АНАЛІЗ ПРАКТИКИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ У ДЕРЖАВАХ-ЧЛЕНАХ ЄС
ОСНОВНЫЕ УГРОЗЫ ПОТЕРИ КОММЕРЧЕСКОЙ ТАЙНЫ В СЕТИ ИНТЕРНЕТ И АНАЛИЗ ПРАКТИКИ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЕС
MAIN MENACES OF INFORMATION LEAKAGE OF A COMMERCIAL SECRET ON THE INTERNET AND ANALYSIS OF THE PRACTICE OF PROTECTION OF COMMERCIAL SECRETS IN THE EU MEMBER STATES

Анотація. *Стаття присвячена визначенню основних загроз втрати комерційної таємниці для юридичних та фізичних осіб під час здійснення ними своїх обов'язків на підприємстві, установах організаціях різних форм*

власності. Визначені основні напрямки можливого збереження інформації, що містить комерційну таємницю, що знаходиться у мережі Інтернет. Протягом останніх років все ширше використання перспективних IT-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак. Гарантування стабільного максимально ефективного функціонування та розвитку будь-якого підприємства є основним завданням безпеки його економічної інформації. Найціннішою економічною інформацією є облікова інформація, яка характеризує всі аспекти господарської діяльності. Стає очевидним, що питання кібербезпеки мають бути у порядку денному кожного підприємства незалежно від його масштабів, рівня складності і характеру комерційної діяльності, а також усвідомлені усіма співробітниками підприємства. Багатоплановий підхід до інформаційних ресурсів обумовлює необхідність враховувати такий суттєвий фактор, як функціонування підприємства за умов ринкових відносин, характерною прикметою яких є боротьба між незалежними суб'єктами господарювання на ринку і гостра конкуренція товаровиробників. Боротьба за економічне виживання — закон ринку. Аналіз практики свідчить, що успішне застосування методів і засобів захисту від загроз відтоку інформації багато в чому залежить від правильного вибору, в кожному конкретному випадку, адекватних приборів, пристроїв, апаратури, а також відповідності технічних засобів вимогам допустимості. Застосування технічних засобів, як відомо, можливе, якщо гарантується дотримання правомірності, безпеки, нешкідливості, морально-етичних норм суспільства. Некритичне сприйняття недоліків і переваг того чи іншого методу захисту інформації може призвести до серйозних втрат у розробці технічних рішень забезпечення безпеки інформації в корпоративній мережі установи.

Особливо важливо відзначити, що невдала, на перший погляд, спроба перехоплення випромінених комп'ютером електромагнітних коливань за допомогою радіоелектронних засобів розвідки і водночас виявлення спеціального генератора перешкод дозволяє дійти висновку про наявність у даній установі секретів, що приховуються на професійному рівні.

Ключові слова: *загрози, інформація, комерційна таємниця у мережі Інтернет, інтелектуальна власність, захист комерційної таємниці, інвестування.*

Аннотация. *Статья посвящена определению основных угроз потери коммерческой тайны для юридических и физических лиц при осуществлении ими своих обязанностей на предприятии, учреждениях организациях различных форм собственности. Определены основные направления возможного сохранения информации, содержащей коммерческую тайну, находится в сети Интернет. В последние годы все более широкое использование перспективных ИТ-технологий обусловило не только многочисленные преимущества, но и целый ряд проблем. В частности, существенно повысился уровень информационного негативного влияния на процессы сохранения и распространения информации, возросла численность новых угроз информационной безопасности, таких как новые формы кибератак. Обеспечение стабильного максимально эффективного функционирования и развития любого предприятия является основной задачей безопасности экономической информации. Ценной экономической информации является учетная информация, характеризующая все аспекты хозяйственной деятельности. Становится очевидным, что вопрос кибербезопасности должны быть в повестке дня каждого предприятия независимо от его масштабов, уровня сложности и характера коммерческой деятельности, а также осознанные всеми сотрудниками предприятия. Многоплановый подход к информационным ресурсам*

обусловливает необходимость учитывать такой существенный фактор, как функционирование предприятия в условиях рыночных отношений, характерной приметой которых является борьба между независимыми субъектами хозяйствования на рынке и острая конкуренция товаропроизводителей. Борьба за экономическое выживание - закон рынка. Анализ практики показывает, что успешное применение методов и средств защиты от угроз оттока информации во многом зависит от правильного выбора, в каждом конкретном случае, адекватных приборов, устройств, аппаратуры, а также соответствия технических средств требованиям допустимости. Применение технических средств, как известно, возможно, если гарантируется соблюдение правомерности, безопасности, безвредности, моральноетичних норм суспильства.Некритичне восприятия недостатков и преимуществ того или иншогометоду защиты информации может привести к серьезным потерям в разработке технических решений обеспечения безопасности информации вкорпоративний сети учреждения. Особенно важно отметить, что неудачная, на первый взгляд, попытка перехвата излучений компьютером электромагнитных колебаний с помощью радиоэлектронных средств разведки и одновременно выявления специального генератора помех позволяет сделать вывод о наличии в данном учреждении секретов, которые скрываются на профессиональном уровне.

Ключевые слова: *угрозы, информация, коммерческая тайна в сети Интернет, интеллектуальная собственность, защита коммерческой тайны, инвестирования.*

Summary. *The article is devoted to identifying the main threats to the loss of trade secrets for legal entities and individuals in the performance of their duties at the enterprise, institutions, organizations of various forms of ownership. The main directions of possible storage of information containing a trade secret on the Internet are identified. In recent years, the increasing use of advanced IT*

technologies has led not only to many benefits, but also a number of problems. In particular, the level of information negative impact on the processes of storage and dissemination of information has significantly increased, the number of new threats to information security, such as new forms of cyberattacks, has increased. Ensuring the stable maximum efficient operation and development of any enterprise is the main task of security of its economic information. The most valuable economic information is accounting information that characterizes all aspects of economic activity. It is becoming clear that cybersecurity issues should be on the agenda of every company, regardless of its scale, level of complexity and nature of business, as well as aware of all employees of the company. The multifaceted approach to information resources necessitates the consideration of such an important factor as the functioning of the enterprise in market relations, a characteristic feature of which is the struggle between independent entities in the market and fierce competition between producers. The struggle for economic survival is the law of the market. Analysis of practice shows that the successful application of the method of protection against threats to the outflow of information largely depends on the correct choice, in each case, of adequate instruments, devices, equipment, as well as the compliance of technical means with the requirements of admissibility. The use of technical means, as is known, is possible if the legality, security, safety, moral and ethical norms of society are guaranteed. Uncritical perception of the disadvantages and advantages of a method of information protection can lead to serious losses in development of technical solutions for information security in corporate network. It is especially important to note that the seemingly unsuccessful attempt to intercept computer-generated electromagnetic oscillations with the help of electronic intelligence and at the same time detect a special interference generator suggests that the institution has secrets hidden at a professional level.

Key words: *threats, information, trade secret on the Internet, intellectual property, protection of trade secret, investment.*

Актуальність досліджуваної тематики. Актуальність статті обумовлена тим, що у світі сучасної комерції інформація є одним з найбільш значущих елементів будь-якого бізнесу. Інформація часто є не тільки джерелом відомостей про фірму або проект, а і товаром, який продають і купують. Втрата навіть частини такої інформації, що міститься у мережі Інтернет веде до великих неприємностей, наслідком чого може стати втрата бізнесу або банкрутства фірми. Під час дослідження даної тематики ми задалися питанням - Які ж загрози існують для інформації? По-перше, загрозу для інформаційної безпеки фірми представляють різного роду електронні «начинки» технічних пристроїв, що застосовуються, частіше за все для копіювання конфіденційної інформації, яка в подальшому буде розміщена у мережі Інтернет. По-друге, безпосередню небезпеку для інформаційного простору будь-якої фірми являють собою самі співробітники компанії. Тому велике значення має внутрішньофірмовий контроль над його співробітниками під час здійснення ними своїх посадових обов'язків. По-третє, існує велика кількість різноманітних програм, розроблених для добування інформації з комп'ютерних мереж і з серверів компаній. Захист інформації, в даному випадку, від несанкціонованого проникнення кібершпигунів дуже важлива. Сама втрата інформації може бути непомітною, а ось наслідки можуть бути катастрофічними.

Стан дослідження проблематики. Вже досить тривалий час правова природа комерційної таємниці, що розміщена у мережі Інтернет та питання визначення основних загроз її втрати була предметом наукових дискусій зарубіжних і вітчизняних учених, серед яких: Ю. Носік [1], Л. Топалова [2], Г. і С. Нікіфорови [3], Е. Соловйов [4] та інші. Ці напрацювання знайшли своє продовження в дослідженні економічної сутності комерційної таємниці та питаннях розроблення механізмів її захисту, що почали аналізуватися у працях Г. Андрощука, П. Крайнєва [5], В. Сідака [6] та інших представників вітчизняної і зарубіжної економічної думки.

Метою статі є дослідження загроз комерційній таємниці у наслідок зростанням технологічних методик та схем у ІТ-сфері, що знайшло свій прояв у розповсюдженні конфіденційної інформації про суб'єктів господарювання та звичайних осіб через її розповсюдження у мережі Інтернет, а також аналіз практики захисту комерційної таємниці в державах-членах ЄС.

Виклад основного матеріалу. В Україні, як і в інших країнах світу, в процесі підприємницької діяльності, при створенні нових технологій, що є наслідком інтелектуальної праці виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, які мають комерційну цінність. Це можуть бути різні методики, перспективні технічні вирішення, результати маркетингових досліджень тощо, спрямовані на досягнення підприємницького успіху.

Протягом останніх років все ширше використання перспективних ІТ-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак.

Інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його життєдіяльності, а процес створення, накопичення, збереження, передачі та обробки, у свою чергу, стимулював прогрес в галузі знарядь її виробництва, що включає електронно-обчислювальну техніку, засоби телекомунікації та системи зв'язку. У зв'язку з новими інформаційними досягненнями державні кордони практично стають прозорими для обігу інформації. При цьому, чим більше зазначена галузь залучається у комерційного обігу, тим більша є потреба в захисті інтересів власників комерційної таємниці. Зрозуміло, комп'ютерні технології - не єдина загроза комерційній таємниці. За підрахунками американських фахівців втрата 20% інформації, що складає комерційну таємницю, веде до банкрутства організації протягом місяця в 60 випадках зі 100 [7]. Отже, у

ринковій економіці інформація стає товаром і її отримання, збереження, передача та використання повинні підпорядковуватися законам товарно-грошових відносин, тобто інформація стає об'єктом та інструментом управління.

Гарантування стабільного максимально ефективного функціонування та розвитку будь-якого підприємства є основним завданням безпеки його економічної інформації. На нашу думку, найціннішою та найактуальнішою економічною інформацією є інформація, що розміщена у мережі Інтернет, яка, в свою чергу, характеризує всі аспекти господарської діяльності. Сьогодні більшість суб'єктів господарювання використовують комп'ютеризовану форму ведення обліку будь-якої інформації, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо. Тому головним пріоритетом захисту інформації на підприємстві є розроблення заходів, спрямованих на збереження інформації, що в подальшому може бути розміщена у мережі Інтернет.

У зв'язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки.

Так С.М. Деньга та Ю.А. Верига виділяють такі дві категорії загроз комерційної інформації, що розміщуються, у тому числі, мережі Інтернет, як активні і пасивні. Активні загрози включають комп'ютерне шахрайство та комп'ютерний саботаж. Пасивні загрози – це помилки системи (пошкодження окремих компонентів обладнання) та катастрофи [8].

Дослідники вказують, що 45% причин виникнення кризового стану становлять навмисні дії.

Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. При цьому низький рівень взаємодії органів державної влади, неурядових організацій та приватного сектору, а також відсутність системних нормативних документів, які описували б загрози Україні в кіберпросторі, є наслідком відсутності цілісного обговорення кібербезпекових питань, пов'язаних, у першу чергу, з захистом комерційної таємниці у мережі Інтернет.

Все вищезазначене дає підставу стверджувати про необхідність провадження у практику правозастосування захисного механізму. Тому, за для цього проаналізуємо практику захисту комерційної таємниці, що розміщується у мережі Інтернет в державах-членах ЄС та спробуємо сформувати певні пропозиції впровадження цього досвіду до діючого законодавства України.

Так, процес європейської інтеграції за змістом є не просто міжнародною взаємодією економік України та ЄС, а насамперед процесом глибокого проникнення інститутів Євросоюзу (законодавства, норм і правил ведення бізнесу, кращих практик тощо) в українську економіку.

Угода про асоціацію між Україною і ЄС містить положення про створення поглибленої та всеохоплюючої зони вільної торгівлі (далі − ПВЗВТ). Відповідно, їх реалізація справить відчутний вплив на українську економіку.

Асоціація з ЄС і створення ПВЗВТ відкриває для підприємств України численні можливості, серед яких: лібералізація торгівлі, інвестиційних потоків і міграції трудових ресурсів. Інтеграція України в європейський ринок означатиме: значне розширення прав споживчого вибору на внутрішньому ринку, оскільки пропозиція товарів і послуг на ньому буде наближатися до структури пропозиції на єдиному ринку ЄС; можливість

зниження цін на окремі групи товарів і послуг як внаслідок зростання конкуренції на внутрішньому ринку, так і внаслідок скасування або зменшення митних платежів; посилення в умовах зростаючої конкуренції стимулів до модернізації та інновацій у середовищі вітчизняних виробників. Положеннями ПВЗВТ передбачено відкриття більшості секторів економіки, що може значно полегшити доступ на ринок ЄС для українських виробників. Крім того, ПВЗВТ передбачає впровадження національного режиму стосовно взаємного інвестування, що повинно значно спростити режим інвестування, насамперед прямих інвестицій.

Як показало дослідження, в Європейському Союзі високий рівень конкурентоспроможності досягається в основному за рахунок використання інноваційних технологій. У свою чергу, інновації, що створюють конкурентні переваги, і є комерційними секретами європейських підприємств. У сучасній європейській економіці комерційна таємниця здебільшого розглядається як результат інвестицій у сферу досліджень та розробок (англ. research and development, надалі – R&D). Існує й інша інформація, що становить комерційну таємницю підприємства, яка не відноситься до R&D (наприклад, списки клієнтів, дані про продажі, маркетингова інформація), однак саме R&D свідчать про інвестиції в нові ідеї, методи, інструменти – і це, здебільшого, є ключовим для віднесення інформації до категорії «комерційна таємниця». Наприклад, з початку 1980-х років витрати США на R&D перевищили 2,5% ВВП. Американський уряд називає цифру в 414 блн. дол., або 2,7% ВВП у 2011 р. [9].

Глобальні інвестиційні тенденції R&D подібні американській спільноті. Саме розмір інвестицій у сферу R&D спонукав європейців до створення єдиного надійного правового середовища для захисту прав інтелектуальної власності, зокрема комерційної таємниці. Попри те, що в ЄС діє Угода про торговельні аспекти прав інтелектуальної власності 1994 р. (Угода ТРІПС), яка стала основою правового захисту комерційної таємниці,

у тому числі, що розміщена у мережі Інтернет, прийняті норми є лише загальними орієнтиром, а тому не досить ефективно виконують призначення, що полягає в досягненні єдності в розумінні питання захисту комерційної таємниці в країнах Євросоюзу. Основною причиною цього є те, що положення Угоди ТРІПС не були повністю імплементовані в національні законодавства країн-учасниць, або імплементовані, але з окремими поправками чи особливостями реалізації.

У рамках ЄС лише Швеція має спеціальне законодавство про комерційну таємницю. В інших країнах норми про комерційну таємницю включені до інших положень законодавства (цивільного, кримінального, конкурентного тощо). В Австрії, Польщі та Іспанії захист комерційної таємниці здійснюється нормами законодавства про недобросовісну конкуренцію, в Італії та Португалії відповідні положення включено до змісту кодексів промислової власності. У Франції конкретні положення про захист виробничих секретів також містяться в кодексі промислової власності. Деліктне законодавство для захисту комерційної таємниці використовується в Нідерландах і Люксембурзі. Принципи деліктного права використовуються переважно для оцінки прямих збитків від втрати комерційної таємниці, а також упущеної вигоди.

У країнах загального права, таких як Велика Британія та Ірландія, які не мають спеціальних законодавчих актів, торгові секрети захищаються загальними нормами контрактного права. Схожі інструменти захисту використовуються на Мальті.

В Україні на сьогодні також відсутнє спеціальне законодавство, яке б регулював захист комерційної таємниці, розміщеної у мережі Інтернет, що, в свою чергу, є перешкодою на шляху створення дієвих механізмів убезпечення комерційної таємниці. При цьому, наявні напрацювання в цій сфері (пропоновані законопроекти) не дають підстав для твердження, що найближчим часом ситуація може змінитися.

У процесі ведення звичайної господарської діяльності суб'єкти підприємництва безвинятково зазнають впливу оточуючого середовища, у тому числі негативного, що безпосередньо чи опосередковано дестабілізує економічний стан підприємства. Процес євроінтеграції, безумовно, вплине на ці фактори. З'являться нові небезпеки як усередині країни, так і ззовні. Особливо це характерно для представників приватного сектору бізнесу, які повинні самостійно протидіяти загрозам їх бізнесу. У зв'язку з цим і постає питання про загрози комерційній таємниці, оскільки такі загрози можуть виражатися у втратах: фінансових, майнових, іміджевих, людських тощо.

Під загрозами комерційній таємниці підприємства, що розміщується у мережі Інтернет, можна розуміти окремі явища, події, процеси, настання (плинність, побічний результат) яких може вплинути на захищеність комерційної таємниці підприємства та привести до негативних наслідків (прямих збитків, неодержаного прибутку, підриву іміджу, зміни в планах, часових втрат тощо). Загрози комерційній таємниці підприємства мають свою специфіку, і це обумовлено, насамперед, таким:

1) посиленням конкурентної боротьби. Комерційна таємниця, будучи інструментом успішного бізнесу та створюючи переваги у веденні підприємницької діяльності, є об'єктом зазіхань з боку конкурентів, які, заволодівши нею, прагнуть або вивести конкурента з ринку, або використати у власній підприємницькій діяльності. Обидва варіанти передбачають негативні наслідки для власника комерційної таємниці у вигляді майнових або немайнових втрат;

2) недосконалістю чинного законодавства;

3) відсутністю досвіду в розробленні та реалізації засобів і методів захисту економічної безпеки підприємства. Наука про економічну безпеку підприємства є молодою, тому підприємства створюють системи економічної безпеки підприємств, здебільшого, керуючись власними уявленнями про її побудову та захист, іноді переймаючи досвід іноземних фірм, при цьому не

беручи до уваги особливості національного середовища. Відсутність досвіду призводить до того, що життєво важливі інтереси підприємства залишаються незахищеними від загроз і можуть зазнати непрогнозованого негативного впливу;

4) відсутністю досвідчених фахівців у сфері захисту комерційної таємниці. Це також впливає на ефективність системи економічної безпеки підприємства з наведених вище причин;

5) невирішеністю соціальних проблем населення (низький рівень доходів, високий рівень безробіття, плинність кадрів тощо). Наведені фактори впливають на ступінь відповідальності працівників за збереження комерційної таємниці підприємства. Адже працівник із посередніми доходами та в пошуках кращого місця роботи не вмотивований зберігати секрети підприємства і є загрозою їх втрати

Інформація, що містить комерційну таємницю, розміщена у мережі Інтернет, постійно піддається різноманітним загрозам. Заходи щодо забезпечення безпеки підприємства повинні бути спрямовані, у тому числі, на виключення або мінімізацію ризиків втрати цінної для підприємства інформації, яка знаходиться у мережі Інтернет, та несанкціонованого доступу до неї. Реалізація цих заходів повинна забезпечувати не тільки безпеку комерційній таємниці, а й сприяти стабільному (сталому) розвиткові підприємства, збільшенню його доходів або досягнення іншої мети.

Висновки. На підставі проведеного дослідження можна дійти висновку, що комерційна таємниця – це навмисно приховувані з комерційних міркувань економічні інтереси та відомості про різноманітні сторони та сфери виробничої, господарської, управлінської, науково-технічної, фінансової діяльності, охорона яких обумовлена інтересами конкуренції та можливими загрозами економічній безпеці.

Способом досягнення економічної безпеки підприємства є ефективне функціонування інформаційної безпеки, засобом якої є впровадження

Положення про захист комерційної таємниці, розміщеної у мережі Інтернет, яке гарантує захист інформаційних ресурсів від несанкціонованого доступу чи використання зацікавленими структурами та особами. Виходячи з того, що ринок засобів і технологій економічної безпеки наповнюється та стає більш диверсифікованим та відбувається активне формування ринкових відносин перехідного періоду, здійснюється імпорт капіталу та технологій, учасники ринку мають формувати більш інтелектуальні засоби забезпечення комерційно-інформаційної безпеки, доповнювати засоби фізичної безпеки їхніми більш цивілізованими різновидами, включаючи технічні та юридичні засоби, до яких належить інститут комерційної таємниці.

Проблеми безпеки комерційної інформації необхідно вирішувати із застосуванням системного підходу: в поєднанні з загальноекономічними, контрольними та правоохоронними механізмами. Прогнозуючи та оцінюючи вплив очікуваних загроз необхідним є створення механізму забезпечення організації безпеки обліковій інформації.

В даному механізмі необхідно врахувати реальну взаємодію підприємства з внутрішнім та зовнішнім середовищем, як наслідок, механізм повинен відображати всю господарську діяльність підприємства.

Що ж стосується аналізу практики захисту комерційної таємниці у мережі Інтернет у країнах ЄС, то можна сказати наступне: як показало дослідження, національні тенденції не відповідають світовим і європейським зокрема – інститут комерційної таємниці досі не розглядається національними підприємствами як елемент розвитку їх інноваційності, а також інвестиційної привабливості за рахунок створення ефективних систем захисту комерційних секретів, що, у першу чергу, забезпечить конкурентоспроможність підприємства.

Такий стан справ негативно позначатися й на реалізації можливостей, що відкриваються для України в процесі євроінтеграції: національні підприємства не зможуть на рівних конкурувати з іноземними інноваційними

компаніями (як на внутрішньому, так і зовнішньому ринках), що вже створили дієві системи захисту комерційної таємниці, яка забезпечує їх ринкові переваги, − з одного боку, а з іншого – формувати привабливий інвестиційний клімат можна лише під гарантії ефективного захисту вкладень.

Наведене вище обумовлює необхідність в умовах перехідного періоду створювати комплексні системи захисту комерційної таємниці, розміщеної у системі Інтернет, в системі економічної безпеки підприємств з тим, щоб уникнути подальших економічних втрат, у тому числі через втрату позицій на ринку.

Література

1. Носік Ю. В. Права на комерційну таємницю в Україні: Монографія К.: КНТ, 2007. 240 с.
2. Топалова Л. Д. Правовий режим комерційної таємниці: автореф. дис. … канд. юрид. наук: спец. 12.00.04 «Господарське право, господарсько-процесуальне право» Донецьк: Інститут економіко-правових досліджень НАН України, 2006.
3. Нікіфоров Г. К. Підприємництво та правовий захист комерційної таємниці: Навч.- практ. посіб. для вищих навч. закл. К.: Олан, 2001. 208 с.
4. Соловьев Э. Коммерческая тайна и ее защита: ЗАО «Бизнес-школа «Интел-Синтез», 1997. 96 с.
5. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны. Монография К.: Издательский дом «ИнЮре», 2000. 400 с.
6. Кадрова безпека суб’єктів господарської діяльності: менеджмент інсайдерами: Монографія / за ред. проф. В. С. Сідака, проф. І. П. Мігус. Черкаси : ТОВ «МАКЛАУТ» Черкаси, 2012. 256 с

7. Бондар О. В. Ситуаційний менеджмент. Навч. посіб.2-ге вид., перероб та доповн. К.: Центр учбової літератури, 2012. 388 с.
8. Безкоровайный М.М. Кибербезопасность – подходы к определению понятия: Вопросы кибербезопасности. № 1(2). 2014. С. 22-27.
9. 2013 Global R&D Funding Forecasts. URL: http://www.rdmag.com/sites/rdmag.com/files/GFF2013Final2013_reduced.pdf

References

1. Nosik Yu. V. Prava na komercijnu tayemnicyu v Ukrayini: Monografiya K.: KNT, 2007. 240 s.
2. Topalova L. D. Pravovij rezhim komercijnoyi tayemnici: avtoref. dis. … kand. yurid. nauk: spec. 12.00.04 «Gospodarske pravo, gospodarsko-procesualne pravo» Doneck: Institut ekonomiko-pravovih doslidzhen NAN Ukrayini, 2006.
3. Nikiforov G. K. Pidpriyemnictvo ta pravovij zahist komercijnoyi tayemnici: Navch.- prakt. posib. dlya vishih navch. zakl. K.: Olan, 2001. 208 s.
4. Solovev E. Kommercheskaya tajna i ee zashita: ZAO «Biznes-shkola «Intel-Sintez», 1997. 96 s.
5. Androshuk G. A. Ekonomicheskaya bezopasnost predpriyatiya: zashita kommercheskoj tajny. Monografiya K.: Izdatelskij dom «InYure», 2000. 400 s.
6. Kadrova bezpeka sub'yektiv gospodarskoyi diyalnosti: menedzhment insajderami: Monografiya / za red. prof. V. S. Sidaka, prof. I. P. Migus. Cherkasi : TOV «MAKLAUT» Cherkasi, 2012. 256 s
7. Bondar O. V. Situacijnij menedzhment. Navch. posib.2-ge vid., pererob ta dopovn. K.: Centr uchbovoyi literaturi, 2012. 388 s.
8. Bezkorovajnyj M.M. Kiberbezopasnost – podhody k opredeleniyu ponyatiya: Voprosy kiberbezopasnosti. № 1(2). 2014. S. 22-27.

9. 2013 Global R&D Funding Forecasts. URL: http://www.rdmag.com/sites/rdmag.com/files/GFF2013Final2013_reduced.pdf