УДК 001.102:34:004
DOI https://doi.org/10.32838/TNU-2707-0581/2020.3/24

Перун Т.С.
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: НОВІ ЗАГРОЗИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У статті досліджено вітчизняний та зарубіжний досвід забезпечення інформаційної безпеки суб'єктів господарювання у процесі здійснення ними своєї виробничої діяльності. Запропоновано різні варіанти його ефективного застосування в Україні. Незважаючи на впровадження у національне законодавство механізмів забезпечення інформаційної безпеки суб'єктів господарювання, не всі проблеми у зазначеній сфері вирішені. Отже, ми вважаємо, що питання, які стосуються захисту суб'єктів господарювання, пов'язані із законодавством, у якому відсутня чітка система захисту інформації та кращий зарубіжний досвід подолання цих проблем.

Тому в сучасному світі інформація є основним товаром, а інформаційна безпека – основою національної безпеки. Для України, яка декларує свої прагнення щодо вступу до Європейського Співтовариства, особливо важливим є приведення положень законодавства у відповідність до європейських стандартів захисту інформації, що передбачає прийняття нового законодавства, вдосконалення та внесення змін до чинних законів на основі впровадження передового досвіду зарубіжних країн з урахуванням національних особливостей законодавства України.

В умовах розвитку економічної конкуренції значного поширення набули такі незаконні явища, як прослуховування, викрадення комерційної інформації на матеріально-речових носіях, вилучення інформації з технічних каналів зв'язку через комп'ютерні мережі. Складнощі перехідного періоду зумовлюють виникнення комплексу невирішених проблем, що обмежують економічний розвиток українських підприємств.

Тому автор статті пропонує вирішення проблем інформаційної безпеки підприємств шляхом прийняття Закону України про комерційну таємницю. Закон повинен містити визначення, види, принципи забезпечення зберігання комерційної таємниці суб'єктів господарювання

Ключові слова: *захист інформації, суб'єкти господарювання, зарубіжний досвід інформаційної безпеки в підприємництві.*

Постановка проблеми. Процес успішного функціонування й економічного розвитку суб'єктів господарювання залежить від якісних та ефективних управлінських рішень, які приймаються на основі детального та всебічного аналізу інформації. Останнім часом у зв'язку з активним розвитком інформаційних технологій та тотальною інформатизацією господарських відносин зростає роль інформації не тільки для розвитку економічного сектору, але і для суспільства загалом. Інформація стала базовим ресурсом публічного управління поряд із людськими, фінансовими та матеріальними ресурсами. Її мобілізація та використання закладені в основу ефективного функціонування і розвитку суб'єктів господарювання.

Із зростанням ролі інформації з'явився інформаційний простір, який потрібно захистити від несанкціонованих чи випадкових наслідків на державному, регіональному рівні чи навіть на рівні окремих підприємств. В економічній діяльності захист інформації може давати можливість отримувати високий дохід, укладати вигідні контракти з контрагентами, значно підвищувати конкурентоспроможність підприємств та ефективність всієї організації. У зв'язку з цим інформаційна безпека є невід'ємною складовою частиною системи державної економічної безпеки.

З розвитком інформаційного суспільства та перетворенням його у сферу діяльності більшості господарюючих суб'єктів усі основні компоненти інформації та інформаційні процеси набувають усе більшого значення. Саме тому в умовах економічної конкуренції інформація нерідко стає об'єктом підвищеного інтересу і навіть злочинних посягань. У таких ситуаціях комплексна інформаційна безпека суб'єкта господарювання виступає гарантом забезпечення економічної безпеки підприємства.

Аналіз останніх досліджень і публікацій. Проблематика правового забезпечення безпеки суб'єктів господарювання (підприємств) різних форм власності висвітлюється у наукових пра-

цях таких учених, як: І.М. Близнюк, О.Р. Братель, В.О. Бондаренко, Jeh C. Johnson., О.М. Ляшенко, R. Latham, Г.В. Козаченко, В.В. Остроухов, В.П. Пономарьов, А.А. Стрельцов, В.Л. Цимбалюк, Т.І. Чубарук, В.М. Щербина та інші. Зокрема, важливий внесок у дослідження інформаційних систем та технологій у системах обліку суб'єктів господарювання зробили такі вчені, як: М.М. Бенько, С.В. Івахненков, B. Sommestad, T. Hallberg, J. Lundholm, K. Bengtsson, В.Д. Шквір та інші. Однак, попри наявність значної кількості наукових праць та актуальність досліджуваних питань, недостатньо дослідженими залишаються наукові підходи до формування правових механізмів забезпечення інформаційної безпеки господарюючих суб'єктів у сучасних умовах, особливо в умовах економічної кризи.

Постановка завдання. Метою статті є детальний аналіз концептуальних та організаційних основ адміністративно-правового забезпечення інформаційної безпеки суб'єктів господарювання та вироблення на зазначеній основі пропозицій і рекомендацій для підвищення ефективності інформаційної безпеки підприємств.

Виклад основного матеріалу дослідження. Під час переходу до ринкових відносин конкуренція серед суб'єктів господарювання зростає, а рівень конкурентоспроможності залежить також від здатності окремих суб'єктів захищати свою комерційну таємницю від зловживань. Тому є нагальна потреба у правовій охороні комерційної таємниці, оскільки її оприлюднення може бути шкідливим, ому що в Україні досі немає повноцінного правового механізму захисту такої інформації.

Крім того, у сучасній юридичній науці детермінації поняття «інформаційна безпека підприємництва» приділено недостатньо уваги, свідченням чого є прогалини у дослідженнях методів інформаційного впливу на діяльність суб'єктів господарювання. Важливою сферою інформаційної безпеки підприємства є протидія інформаційно-психологічному впливу. З розвитком інформаційних технологій вдосконалено методи інформаційного впливу на суспільство чи окремих людей, технології маніпуляції поширюються на відносини у сфері господарювання і значно випереджають розвиток засобів та методів протидії такому впливу. Це може призвести до погіршення економічного розвитку та розбалансування суспільних процесів [1].

Слід розуміти, що протистояння інформаційному та психологічному впливу розглядається як один з інструментів інформаційного протистояння або його пікової стадії – інформаційної війни ринкових монополістів.

Окрім цього, сьогодні ще не регламентовані державними нормативно-правовими актами організація та методи конфіденційного комерційного діловодства. Їх має право визначати власник конфіденційної інформації, керуючись власним досвідом та спеціалізацією приватного підприємства. Тому необхідність забезпечення належного рівня функціонування підприємства, збереження конфіденційної інформації та належного зберігання таких документів зумовлює необхідність прийняття загальнодержавних стандартів, норм та правил роботи з конфіденційними документами.

Саме недосконаліть чинного законодавства створює проблеми для власників комерційної таємниці, а також обмежує можливість захисту їхніх прав на таку інформацію. У нашій державі відсутнє визначення правового положення комерційної таємниці як соціального та фінансового ресурсу, юридичне закріплення права на комерційну таємницю та створення законодавчих гарантій захисту цього права, регулювання відносин, які виникають у сфері обігу комерційної таємниці, через це відбувається поширення комерційного шпіонажу та безперешкодне незаконне використання комерційної таємниці.

У нашій країні керівництво компанії може на власний розсуд створити окремий департамент (відділ) інформаційної безпеки, в обов'язки якого входить контроль за розповсюдженням інформації, що становить комерційну таємницю.

Для того, щоб певна інформація набула статусу комерційної таємниці суб'єкта господарювання, він повинен легалізувати інформацію з метою здійснення свого права на комерційну таємницю та її захисту від розголошення. Право на комерційну таємницю може бути закріплено в статуті підприємства, колективному договорі, правилах внутрішнього трудового розпорядку, положенні про комерційну таємницю тощо [2].

Щоб запобігти розголошенню комерційної таємниці, слід спочатку захистити себе на нормативному рівні від розголошення співробітниками компанії. Адже домінуючим завжди буде людський фактор: співробітники – це наймані працівники, а отже, можуть неодноразово змінити місце роботи. А за наявності відкритого доступу до комерційної таємниці підприємства вони можуть використати її у своїх інтересах, а також передати її третім особам, що може завдати господарюючому суб'єкту істотної шкоди.

Одним із найбільш ефективних механізмів захисту комерційної таємниці є укладення угоди про нерозголошення (NDA). При цьому підприємству доцільно розробити та прийняти Положення про комерційну таємницю та затвердити його наказом керівника або доповнити умови трудового договору положенням про нерозголошення і просто письмово засвідчити ознайомлення співробітника з положенням [3; с. 42].

Тоді в трудовому договорі досить зафіксувати обов'язок не розголошувати комерційну таємницю і передбачити відповідальність за її розголошення відповідно до чинного законодавства та положення про комерційну таємницю (рис. 1).

Щодо захисту комерційної таємниці від потенційного розголошення у відносинах із контрагентами, то тут під найбільшим ризиком угоди, пов'язані з розробленням маркетингових кампаній, здійсненням соціологічних досліджень ринку з метою реалізації нових товарів, інноваційною, фінансовою, лізинговою та інвестиційною діяльністю.

Такий ризик зумовлений тим, що зазначені правовідносини передбачають повідомлення контрагенту інформації, що становить комерційну таємницю. Тому перед наданням інформації, що містить комерційну таємницю для іншої сторони, доцільною є формалізація зобов'язань щодо конфіденційності іншої сторони. Юридична фіксація зобов'язання можлива шляхом укладення з контрагентом угоди про нерозголошення (NDA).

У будь-якому разі порядок розголошення третім особам інформації, що становить комерційну таємницю, і порядок повідомлення їм про заборону використання таких відомостей має бути передбачено положенням про комерційну таємницю.

Аналіз практики укладання господарських та цивільних договорів свідчить про те, що сторони часто передбачають у тексті угоди положення про доступ до комерційної таємниці контрагента, посилаючись на положення про комерційну таємницю. Такі дії забезпечують формування юридичного бар'єру для захисту комерційної таємниці сторін договору.

Тому для запобігання розголошенню інформації про комерційну таємницю таку інформацію слід ідентифікувати, встановити свої права, запровадити заходи для забезпечення її захисту і передбачити санкції за розголошення такої інформації, а також проводити роз'яснювальну роботу із співробітниками щодо заборони розголошення комерційної таємниці.

Будь-яка інша інформація вважається відкритою. Захист комерційної таємниці здійснюється відповідно до положень чинного законодавства за дотримання встановлених вимог, а саме виключно в інтересах національної безпеки, захисту територіальної цілісності або протидії порушенням громадського порядку з метою запобігання правопорушенням чи злочинам, для захисту здоров'я населення, прав та законних інтересів інших людей, а також для підтримки авторитету і неупередженості правосуддя. Також оприлюднення комерційної таємниці допустимо, якщо шкода від розголошення такої інформації переважає рівень захисту інтересів суспільства та держави у разі її отримання.

Дослідження особливостей обробки документів, що містять комерційну таємницю, дає змогу виокремити низку основних вимог щодо використання та обліку конфіденційних документів.

Заходи щодо захисту комерційної таємниці можна розділити на три категорії: нормативні,

У положенні про комерційну таємницю варто встановити:

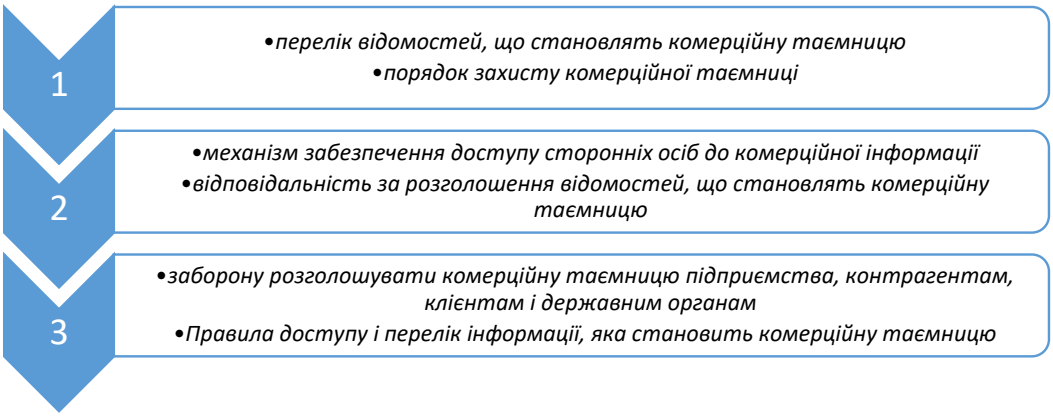

Рис. 1.

організаційні та технічні. Отже, обов'язки щодо охорони комерційної таємниці покладено не лише на її власника (керівника підприємства, для якого ця інформація становить комерційну таємницю), а й на органи публічної влади. Також важливе значення для охорони комерційної таємниці має створення департаменту діловодства на підприємстві, який відповідає за додержання єдиного порядку обліку, використання та зберігання документів. Правопорушення у сфері застосування комерційної таємниці тягнуть за собою дисциплінарну, адміністративну, цивільну та кримінальну відповідальність, передбачену чинним законодавством.

Найбільше значення має дослідження проблем правової регламентації охорони документів, що містять комерційну таємницю. На жаль, окремого Закону України, у якому визначено всі дефініції, встановлено процедуру захисту та систематизовано регламент роботи з інформацією, що містить комерційну таємницю, немає. Проте стаття 21 Закону України «Про інформацію» передбачає, що «відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом» [4].

Цивільний кодекс України, встановлюючи перелік майнових прав, пов'язаних із правом інтелектуальної власності щодо комерційної таємниці (ст. 506), на жаль не передбачає правового механізму захисту комерційної таємниці, порядку встановлення належності інформації до комерційної таємниці, підстав виникнення та припинення прав особи на комерційну таємницю, порядку доступу до комерційної таємниці тощо [5].

Таким чином, удосконалення правового регулювання відносин щодо визначення, поширення, збереження та захисту комерційної таємниці – прерогатива спеціального закону, який нині в Україні так і не прийнято. Відсутність спеціального законодавства позбавляє володільців баз даних, які належать до комерційної таємниці, можливостей для належного захисту своєї інформації, обмежує шляхи реалізації прав особи у сфері використання інформації з обмеженим доступом, яка формується в процесі здійснення господарської діяльності, завдає матеріальної та моральної шкоди власникам комерційної таємниці, що також необхідно передбачити у проекті нового закону.

На інституційному рівні для забезпечення інформаційної безпеки в Україні створено систему органів державної влади та місцевого самоврядування. Так, реалізацію національної політики інформаційної безпеки України здійснюють більше двадцяти державних органів влади. Проте Україна все частіше стикається з масштабними проявами кіберзлочинності, що загрожує ефективному та безпечному функціонуванню економічної системи країни [3].

Водночас в Україні затверджено «Стратегію кібербезпеки України», яка має на меті створення умов для безпечного розвитку кіберпростору та його використання в інтересах суб'єктів господарювання [6].

На доказ цього уряд США у 2016 році вперше офіційно підтвердив, що до порушень у системі забезпечення електричною енергією в Україні у грудні 2015 року призвели дії кіберзлочинців [7]. Крім того, Служба безпеки України у 2015 році повідомляла про викриття хакерської атаки зарубіжних спецслужб проти енергетичних об'єктів на Заході України. Службовці СБУ знайшли несанкціоноване програмне забезпечення в мережах окремих обласних підприємств електроенергетики.

Високий рівень несанкціонованого втручання у кібернетичний простір підтверджено дослідженнями провідного німецького оператора зв'язку Deutsche Telecom, за даними якого Україна перебуває на четвертому місці у світі серед країн, потерпілих від кібератак. Підрозділом CERT-UA, який діє у складі Державної служби спеціального зв'язку та захисту інформації України, виявлено та вжито заходів для запобігання 32 кіберпорушень, які пов'язані з порушенням електронного документообігу державних підприємств.

Найбільш поширеними видами атак є несанкціонований доступ до автоматизованих систем (17 випадків) та DDoS-атаки на державні інформаційні ресурси (6 випадків). Крім того, українська розвідка вжила заходів щодо блокування чи видалення фішинг-вмісту на 150 веб-сайтах української частини мережі Інтернет для усунення несанкціонованого втручання.

Саме ці факти свідчать про необхідність захисту інформаційної безпеки суб'єктів господарювання шляхом прийняття Закону України про комерційну таємницю. Адже потреба у належному інформаційному захисті підприємств зростає з розвитком вітчизняного підприємництва та посиленням конкуренції у товарній ринковій економіці. Є нагальна потреба в узаконенні суспільних відносин, які не підпадають правовій регламентації через комерційну таємницю; відсутні законодавчі акти, необхідні для легалізації суспільних відносин у сфері захисту комерційної таємниці; необхідне приведення

вітчизняного законодавства у сфері захисту комерційної таємниці у відповідність із нормами і стандартами ЄС.

Висновки. У сучасних умовах економічна система розвинутих країн світу та України перебуває у перманентній залежності від ІТ-технологій, кіберпростір охоплює практично всі сфери суспільного життя, насамперед – стратегічні, включаючи сферу публічного управління, оборону держави, альтернативну енергетику, управління державними підприємствами з безперервним циклом виробництва тощо.

Проблематика забезпечення економічної, фінансової та інформаційної безпеки суб'єктів господарювання в Україні на сучасному етапі є дуже актуальною, враховуючи мобілізацію, використання та обмін інформацією, зокрема проведення бухгалтерського обліку, за допомогою іноземних програм (виробництва країни-агресора). Деякі з них містять програмні модулі, за допомогою яких можливе несанкціоноване отримування комерційної інформації, що може використовуватися кіберзлочинцями.

Україна володіє належним потенціалом для захисту інформаційної безпеки господарюючих суб'єктів. Це, зокрема, забезпечують сертифіковані висококласні спеціалісти, які можуть створити конкурентоспроможне експортоорієнтоване середовище. Тому зазначених осіб потрібно активно залучати для створення важливого для забезпечення безпеки країни програмного забезпечення, включаючи програмне забезпечення для бухгалтерського обліку.

На національному рівні необхідно Кабінет міністрів України наділити функціями контролю інформаційного забезпечення виробничих підприємств України, включаючи забезпечення заходів із розвитку державного програмного забезпечення, що застосовується у виробничих компаніях, інфраструктурі, фінансових установах, оборонних установах та інших агенціях, що забезпечують національну безпеку.

На сучасному етапі інформаційна безпека господарюючих суб'єктів різних форм власності може гарантуватися тільки комплексною системою захисту інформації на законодавчому рівні шляхом прийняття Закону України про комерційну таємницю. Закон повинен містити визначення, види принципи забезпечення зберігання комерційної таємниці суб'єктів господарювання.

Список літератури:

1. Latham, R. (2013) *Information Management Advice 35: Implementing Information Security.* Retrieved November 2013, from: https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2035%20Implementing%20Information%20Security%20Part%204%20-%20IS%20Policy.pdf

2. Snedaker, S. (2013). *Business continuity and disaster recovery planning for IT professionals.*USA: Elsevier Inc.

3. Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," Information Management & Computer Security (22:1), pp 42–75.

4. «Про інформацію»: Закон України від 2 жовтня 1992 року№ 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 30.04. 2020).

5. Цивільний кодекс України від 16 січня 2003 року№ 435-IV URL:https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 30.04. 2020).

6. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016 URL: https:// https://zakon.rada.gov.ua/laws/show/n0003525-16 (дата звернення: 18.04. 2020).

7. Statement by Secretary Jeh C. Johnson on H.R. 644, The Trade Facilitation and Trade Enforcement Act of 2015 URL: https://www.dhs.gov/news/2016/02/24/statement-secretary-jeh-c-johnson-hr-644-trade-facilitation-and-trade-enforcement#

Perun T.S. INFORMATION SECURITY OF BUSINESS ENTITIES: NEW THREATS AND PROSPECTS OF DEVELOPMENT

The article explores the domestic and foreign experience of providing information security of economic entities in the course of their production activities. Different variants of its effective application in Ukraine are offered. Despite the introduction of mechanisms for ensuring the information security of economic entities into national law, not all problems in this field have been resolved. Therefore, we believe that the issues related to the protection of business entities are related to the legislation, which lacks a clear system of information protection and better foreign experience in overcoming them.

Therefore, in the modern world, information is a basic commodity, and information security is the basis of national security. For Ukraine, which declares its aspirations to join the European Community, it is especially important to bring the provisions of the legislation in line with the European standards of information protection, which envisages the adoption of new legislation, improvement and amending of the existing laws based on the implementation of best practices of foreign countries from abroad features of the legislation of Ukraine.

In the context of economic competition, such illegal phenomena as listening, theft of commercial information on physical media, the removal of information from technical communication channels through computer networks became widespread. The complexities of the transition period lead to the emergence of a complex of unresolved problems that limit the economic development of Ukrainian enterprises.

Therefore, the author proposes to solve the problems of information securityenterprises, through the adoption of the Law of Ukraine on trade secrets. The law should contain definitions, types of principles for securing the business secrecy of economic entities

Key words: *information protection, business entities, foreign experience of information security in business.*