УДК 340
DOI https://doi.org/10.32782/pdu.2024.3.8

М. О. Шевчук
кандидат юридичних наук,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права імені Леоніда Юзькова
orcid.org/0000-0001-7549-6344

ПРАВОВЕ РЕГУЛЮВАННЯ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стаття присвячена питанням інформаційної безпеки, яка визначається як рівень захищеності держави та стійкості її основних сфер життєдіяльності від небезпечних інформаційних впливів. У сучасному світі безпека інформаційного простору є критично важливою, адже вона впливає на ефективність функціонування економіки, науки, техносфери, управління та військової справи. У статті розглядаються різноманітні джерела загроз, які можуть походити як від окремих осіб, так і від організацій, створюючи спектр інформаційних ризиків для держави та суспільства. У тексті акцентується увага на значенні забезпечення інформаційної безпеки в контексті підприємницької діяльності, адже актуальна і достовірна інформація стала ключовим ресурсом для розвитку суспільства.

Також у роботі аналізується поточний стан досліджень у цій сфері, зокрема, недостатня увага до розробки спеціалізованих інструментів для забезпечення інформаційної безпеки підприємств. Визначено основні загрози для сучасних підприємств, серед яких незаконна діяльність, порушення норм обробки даних та помилки персоналу. Акцентується на важливості комплексного підходу до забезпечення інформаційної безпеки через організацію державної системи, яка включає в себе державні органи та інші структури, а також принципи законності, взаємної відповідальності та інтеграції національних систем безпеки з міжнародними. Наведена інформація завершується висновками про необхідність удосконалення правової бази та впровадження превентивних заходів для ефективного захисту інформаційного простору.

Ключові слова: *інформаційна безпека, рівень захищеності, сфери життєдіяльності, небезпечні інформаційні впливи, ефективність функціонування, економіка, наука, управління, військова справа, джерела загроз, інформаційні ризики, підприємницька діяльність, актуальна інформація, достовірна інформація, дослідження, спеціалізовані інструменти, незаконна діяльність, порушення норм обробки даних, помилки персоналу, комплексний підхід, державна система, принципи законності, взаємна відповідальність, інтеграція національних систем безпеки, правова база, превентивні заходи, захист інформаційного простору.*

Постановка проблеми. Інформаційна безпека характеризується рівнем захищеності держави та стійкістю основних сфер її життєдіяльності (економіка, наука, техносфера, управління, військова справа тощо) від небезпечних інформаційних впливів, які можуть дестабілізувати або завдати шкоди державним інтересам. Це стосується як впровадження, так і витоку інформації. Здатність держави протидіяти таким впливам визначає рівень її інформаційної безпеки. Джерелами загроз можуть бути як окремі особи, так і організації або їх об'єднання. Разом вони створюють спектр інформаційних загроз, що впливають на рівень інформованості окремих громадян, суспільства та держави в цілому.

Забезпечення інформаційної безпеки підприємницької діяльності є одним із важливих елементів загальної інформаційної безпеки держави. Сьогодні актуальна та достовірна інформація стала важливим фактором виробництва, розглядаючись як один із основних ресурсів розвитку суспільства. Разом із розвитком та ускладненням засобів, методів і форм автомати-

зації процесів обробки інформації зростає залежність підприємств від рівня безпеки застосовуваних ними інформаційних технологій.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки як складової національної безпеки, а також різні аспекти державного управління і політики щодо захисту національного інформаційного простору досліджували такі науковці, як Ю. С. Шемшученко, І. С. Чиж, О. Ф. Скакун, Т. Субіна, О. Гарагонич, Н. О. Саніахметова. та інші. Однак досі недостатньо досліджені питання розробки спеціалізованих інструментів інформаційної безпеки для підприємницької діяльності, що спрямовані на забезпечення безпеки національної економіки в умовах сучасного цивілізаційного розвитку.

Постановка завдання. Незважаючи на значний внесок у дослідження інформаційної безпеки з боку науковців, залишається недостатньо вивченим аспект захисту підприємницької діяльності, що є важливим для національної економіки. Завдання полягає в тому, щоб розробити спеціалізований інструментарій інформаційної безпеки для підприємств, який відповідатиме сучасним умовам цивілізаційного розвитку та забезпечить ефективну протидію загрозам в інформаційному просторі.

Метою роботи є дослідження сучасних викликів і загроз у сфері інформаційної безпеки підприємницької діяльності та розробка відповідних заходів для їх нейтралізації в умовах цифровізації та глобалізації економічних процесів.

Викладення основного матеріалу. У найзагальнішому сенсі інформаційна безпека – це стан захищеності інформаційного простору суспільства, що гарантує його формування, використання та розвиток в інтересах громадян, організацій і держави. Під інформаційним простором розуміють сферу діяльності, пов’язану зі створенням, обробкою та споживанням інформації. Він умовно поділяється на кілька складових [1]:

– створення і поширення первинної та вторинної інформації; – формування інформаційних ресурсів, підготовка інформаційних продуктів та надання інформаційних послуг; – споживання інформації; – розробка та використання інформаційних систем, технологій і засобів їхнього забезпечення; – створення та впровадження засобів і механізмів забезпечення інформаційної безпеки.

Варто зауважити, що задоволення інформаційних потреб сприяє отриманню знань про навколишній світ і процеси, які в ньому відбуваються, що забезпечує інформованість як особистості, так і суспільства та держави.

Важливу роль у забезпеченні інформаційної безпеки держави відіграє інформаційна безпека підприємницької діяльності. Основними загрозами для інформаційної безпеки сучасного підприємства є: незаконна діяльність окремих економічних суб'єктів у сфері створення, поширення та використання інформації; порушення встановлених правил збору, обробки та передачі даних; навмисні дії чи ненавмисні помилки персоналу інформаційних систем; помилки в проєктуванні інформаційних систем; технічні збої і проблеми з програмним забезпеченням у інформаційних і телекомунікаційних системах.

Джерелами негативних впливів на інформаційну безпеку підприємства можуть бути:

1. свідомі або несвідомі дії посадових осіб та суб'єктів господарювання (органи державної влади, міжнародні організації, конкурентні підприємства);

2. об'єктивні чинники (зміни на фінансових ринках, наукові відкриття, технологічні розробки, форс-мажорні обставини).

Залежно від джерела, негативні впливи можуть бути об'єктивними, тобто такими, що виникають без участі конкретного підприємства чи його працівників, або суб'єктивними, що зумовлені неефективною роботою підприємства чи його співробітників (особливо керівництва та функціональних менеджерів).

Мета інформаційної безпеки підприємства полягає в забезпеченні його стабільної та ефективної роботи сьогодні та високого потенціалу розвитку в майбутньому.

Одним із джерел загроз для суспільства в інформаційній сфері є постійне ускладнення інформаційних систем і мереж

критично важливої інфраструктури. Такі загрози можуть включати навмисні або випадкові помилки, збої техніки, відмови програмного забезпечення, а також злочинні дії. Основними цілями таких дій можуть бути енергетичні, транспортні, трубопровідні та інші елементи інфраструктури.

Друге джерело загроз є можливість концентрації засобів масової інформації в руках обмеженого кола власників. Це може призводити до маніпулювання суспільною думкою щодо важливих суспільних подій, а також до підриву моральних цінностей через нав'язування чужорідних ідей.

Ще однією загрозою є зростання масштабів вітчизняної та міжнародної комп'ютерної злочинності. Вона може проявлятися через спроби здійснення шахрайських операцій з використанням глобальних та національних інформаційно-телекомунікаційних систем, відмивання незаконно отриманих коштів, отримання несанкціонованого доступу до фінансових, банківських та інших даних з метою їхнього незаконного використання.

Існує три основні зовнішні джерела загроз для діяльності підприємств. Наприклад, несприятлива економічна політика держави. Регулювання валютного курсу, митних тарифів, податкових ставок та інші економічні заходи можуть вступати в конфлікт з виробничими, комерційними та фінансовими інтересами підприємств. Державні адміністративні дії, зловживання владою, перевищення компетенції у відносинах з підприємствами або незаконне втручання у їхню діяльність також є потенційними загрозами [2, с. 110–113].

Також недобросовісна конкуренція з боку інших суб'єктів господарювання. Вона може проявлятися у спробах представити діяльність одного підприємства як діяльність іншого, поширенні неправдивої інформації для дискредитації конкурента або неправомірному використанні маркувань, що можуть ввести споживача в оману.

Як свідчать міжнародні дані, втрати від промислового шпигунства сягають десятків мільярдів доларів. Наприклад, у США понад 1,5 мільйона людей зайнято в системах захисту конфіденційної інформації приватного сектора, що перевищує кількість працівників державних служб безпеки. Деякі компанії спеціалізуються на промисловому шпигунстві, використовуючи професійні, а часто і незаконні методи для здобуття інформації [1].

Забезпечення інформаційної безпеки включає комплекс заходів, спрямованих на досягнення захищеності інформаційних потреб особистості, суспільства та держави. Держава реалізує ці заходи через відповідні органи, тоді як громадяни діють через громадські організації та об'єднання, що мають відповідні повноваження.

Основою забезпечення інформаційної безпеки держави є такі принципи [4, с. 227–229]:

– законність та дотримання балансу інтересів особистості, суспільства і держави;

– взаємна відповідальність між усіма суб'єктами, що забезпечують інформаційну безпеку;

– інтеграція національних систем безпеки з міжнародними.

Серед специфічних принципів інформаційної безпеки слід відзначити:

– превентивний характер заходів, які проводяться в рамках інформаційної безпеки порівняно з іншими видами безпеки;

– забезпечення достатньої інформованості об'єктів безпеки, включно з міжнародними.

Державна система забезпечення інформаційної безпеки є організаційною структурою, яка об’єднує державні органи, а також сили і засоби інформаційної безпеки, що діють на основі законодавства під наглядом і захистом судової влади. Ця система є ключовою складовою в забезпеченні інформаційної безпеки особистості, суспільства та держави у правовій державі.

Основні завдання цієї системи включають: а) виявлення та прогнозування дестабілізуючих факторів і загроз для життєво важливих інтересів особистості, суспільства та держави; б) реалізацію оперативних і довготривалих заходів для попередження та усунення цих загроз; в) створення і підтримання готовності сил і засобів, необхідних для забезпечення інформаційної безпеки.

Органи інформаційної безпеки можуть бути створені і в недержавних структурах для захисту їхніх інтересів в інформаційній сфері. Вони, на основі відповідних угод, можуть інтегруватися до загальної державної системи інформаційної безпеки.

Наразі окремі елементи цієї системи вже функціонують (зокрема, органи зовнішньої розвідки, інформаційні служби різних міністерств, системи технічного і криптографічного захисту інформації). Однак правова база для їхньої діяльності все ще є недостатньою, а функціонування цих органів не повністю відповідає покладеним на них завданням. Це зумовлено недостатньою опрацюванням питань щодо форм і методів забезпечення інформаційної безпеки.

Форми і методи забезпечення інформаційної безпеки є інструментом, за допомогою якого сили інформаційної безпеки виконують завдання щодо захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне регулювання через розробку відповідних нормативних актів, що регулюють діяльність органів інформаційної безпеки [6, с. 211–212].

Однією з форм забезпечення інформаційної безпеки є інформаційний патронат, який полягає в тому, що держава надає фізичним і юридичним особам інформацію про дестабілізуючі фактори і загрози, а також забезпечує захист їхніх життєво важливих інтересів від цих загроз.

Інформаційне забезпечення інформаційної безпеки охоплює збір, обробку та обмін інформацією про загрози між відповідними органами і силами системи безпеки. Збір необхідних даних здійснюється через розвідувальні, контррозвідувальні та оперативно-інформаційні заходи.

Захист інформації забезпечується шляхом підготовки законодавчих ініціатив, судового захисту та проведення оперативних заходів силами і засобами інформаційної безпеки.

Сьогодні ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, розглядається фахівцями як комплекс заходів, що функціонує в кількох взаємопов'язаних напрямках:

– Захист від злочинних угруповань;

– Запобігання порушенням закону, щоб уникнути можливих санкцій;

– Захист від недобросовісної конкуренції;

– Захист від неправомірних дій з боку власних співробітників.

Враховуючи наявність численних загроз для підприємства, доцільно централізувати всі заходи з безпеки під управлінням єдиного виконавчого органу, що називається «службою (відділом) безпеки». Ця служба здійснює контроль над усіма аспектами діяльності фірми і запроваджує ефективні механізми протидії негативним чинникам. Для цього вона може використовувати власні ресурси, а в деяких випадках – залучати зовнішні організації.

Забезпечення безпеки сучасного комерційного підприємства реалізується через такі режими [3, с. 250–256]:

– Конфіденційність і захист об'єктів інтелектуальної власності, що охоплює інформаційну безпеку;

– Фізична охорона, що забезпечує безпеку майна та персоналу компанії.

В умовах українського ринку підприємець може сподіватися на ефективний захист своїх життєво важливих інтересів лише за умови, що він здатний організувати процес, орієнтований на усунення потенційних загроз. Це передбачає позбавлення супротивника інформації про виробничі та торговельні можливості, насамперед шляхом виявлення і ліквідації індикаторів (демаскуючих ознак та каналів витоку інформації), пов'язаних з плануванням і реалізацією підприємницької діяльності. Важливо, щоб у цьому процесі були задіяні всі співробітники підприємства, а не лише служба безпеки.

Системний підхід до забезпечення інформаційної безпеки полягає у тому, щоб зупинити, зменшити або, в крайньому випадку, обмежити виток цінної інформації, яка може надати конкурентам можливість заздалегідь дізнатися про плани та дії керівництва компанії.

На жаль, в Україні майже повністю бракує необхідних елементів для реалізації такого системного підходу, серед яких [5, с. 88–92]:

– Достатня законодавча база, що регулює основні бізнес-відносини, оскільки

приватне право і юридичне забезпечення економічної діяльності ще недостатньо розвинуті.

– Відпрацьований механізм економічних реформ на загальнодержавному та регіональному рівнях.

– Адекватний рівень залучення суспільства в процеси економічних перетворень.

– Державна програма боротьби з корупцією в національній економіці.

– Ефективна національна статистика та контроль.

Ігнорування законів ринкової економіки та потреб економічної безпеки часто призводить до зриву вигідних угод, укладання контрактів з недобросовісними партнерами, а також прийняття на роботу осіб з низькими моральними стандартами, які можуть стати «підставою» для недобросовісних конкурентів або організованої злочинності. Отже, легше, дешевше і вигідніше підтримувати необхідний рівень економічної безпеки, ніж витрачати час і ресурси на тривалі й нерідко невдалі судові процеси з метою захисту своїх прав.

Висновки та перспективи подальшого розвитку. Таким чином, серед основних механізмів забезпечення інформаційної безпеки підприємницької діяльності в Україні, що є частиною загальної інформаційної безпеки держави, можна виокремити: інформаційний патронат, інформаційний захист (включаючи судовий, адміністративний та автономний), інформаційну кооперацію та формування ефективних систем захисту інформації.

Сьогодні забезпечення безпеки підприємницької діяльності, як і національної економіки загалом, повинно бути організоване в систему заходів, що охоплюють такі взаємопов'язані напрями: захист від злочинних елементів; захист від правопорушень, щоб уникнути санкцій; захист від недобросовісної конкуренції; а також захист від протиправних дій з боку власних співробітників.

Забезпечення інформаційної безпеки підприємницької діяльності в Україні має спиратися на специфічні принципи, такі як превентивний характер заходів і належна інформованість об'єктів безпеки, включаючи міжнародні структури. Такий процес викликає необхідність розробки конкретних механізмів реалізації вказаних принципів, що відкриває перспективи для подальших досліджень у цій галузі. Перспективи розвитку інформаційної безпеки підприємницької діяльності в Україні є дуже актуальними і мають великий потенціал. Перш за все, варто зазначити, що зміцнення законодавчої бази – це один із головних кроків на шляху до забезпечення надійної інформаційної безпеки. Створення чітких правил гри у цій сфері дозволить підприємствам краще захистити свої дані та права від можливих загроз.

Треба поліпшити співпрацю між державними органами, які займаються питаннями інформаційної безпеки. Взаємодія між цими структурами може включати спільні тренінги та обмін досвідом, що дозволить підвищити загальний рівень безпеки. Це важливо, оскільки інформаційні загрози часто мають комплексний характер.

Рекомендується впровадження нових технологій. Сучасні рішення, такі як штучний інтелект, можуть суттєво поліпшити захист інформації. Інвестиції в ці технології допоможуть підприємствам швидше реагувати на загрози і забезпечити безпеку своїх даних.

Також потрібно зосередитися на формуванні культури безпеки в самих підприємствах. Коли співробітники усвідомлюють важливість інформаційної безпеки та активно беруть участь у її забезпеченні, це може суттєво підвищити загальний рівень захисту. Тренінги та навчання можуть допомогти їм краще розуміти, як уникати ризиків.

Обмін досвідом з іншими країнами та партнерство у сфері інформаційної безпеки дозволять Україні запроваджувати найкращі практики, що використовуються у світі. Це може бути корисно не лише для окремих підприємств, а й для всієї національної економіки.

Необхідно запровадити моніторинг та оцінку впроваджених заходів безпеки. Розробка механізмів оцінки стане кроком на шляху до ефективного управління інформаційною безпекою.

Ще можливо подумати про кооперацію між підприємствами. Об’єднання зусиль у сфері інформаційної безпеки дозволить

компаніям ефективніше боротися зі спільними загрозами. Укладення угод про співпрацю дасть можливість ділитися інформацією про загрози та досвідом у їх подоланні.

Загалом, усе вищевикладене, може суттєво підвищити інформаційну безпеку підприємств в Україні. Такі перспективи не лише допоможуть компаніям захистити свої дані, але й зміцнить економіку країни в цілому.

Список використаної літератури:

1. Гарагонич О. Теоретичні питання державного регулювання господарської діяльності / О. Гарагонич. URL: http://bnc.in.ua/ pravovezabezpechennya-gospodarskoi-diyalnosti/teoretichni-pitannyader zhavnogoreguliuvannya-gospodarskoi-diyalnosti/ (дата звернення: 16.10.2024).
2. Е-майбутнє та інформаційне право / за ред. М. Швеця. 2-е вид., доп. Київ: НДЦПІ АПрН України, 2106. 234 с.
3. Правове забезпечення інформаційної діяльності в України / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. Київ : Юридична думка. 2016. 384 с.
4. Саніахметова Н. О. Підприємницьке право: Суб'єкти підприємництва. Кредитування. Оренда. Лізинг. Зовнішньоекономічна діяльність. Інвестиції. Антимонопольне законодавство. Захист від недобросовісної конкуренції. Реклама : навч. посіб. К. : А. С. К., 2011. 704 с.
5. Скакун О.Ф. Теорія держави і права: підручник. Харків: Консул. 2001. 656 с.
6. Субіна Т. Поняття і сутність інформації у просторі держави. *Науковий вісник Національної академії ДПС України*. 2017. № 4 (26). С. 210–213.

Shevchuk M. Legal regulation of the information security mechanism

The article is dedicated to the issues of information security, which is defined as the level of protection of the state and the resilience of its main areas of life from dangerous information influences. In today's world, the security of the information space is critically important, as it affects the effectiveness of the functioning of the economy, science, the techosphere, management, and military affairs. The article discusses various sources of threats that can arise from both individuals and organizations, creating a spectrum of information risks for the state and society.

The text emphasizes the significance of ensuring information security in the context of entrepreneurial activity, as relevant and reliable information has become a key resource for the development of society. The work also analyzes the current state of research in this area, particularly the insufficient attention given to the development of specialized tools for ensuring information security in enterprises.

The main threats to modern enterprises are identified, including illegal activities, violations of data processing norms, and personnel errors. The importance of a comprehensive approach to ensuring information security through the organization of a state system, which includes state bodies and other structures, is highlighted. This approach also encompasses the principles of legality, mutual responsibility, and the integration of national security systems with international ones. The information presented concludes with findings on the necessity of improving the legal framework and implementing preventive measures for the effective protection of the information space.

Key words: *information security, level of protection, spheres of life, dangerous information influences, effectiveness of functioning, economy, science, management, military affairs, sources of threats, information risks, entrepreneurial activity, relevant information, reliable information, research, specialized tools, illegal activities, violations of data processing standards, staff errors, comprehensive approach, state system, principles of legality, mutual responsibility, integration of national security systems, legal framework, preventive measures, protection of the information space.*