РОЗДІЛ VII. АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.6:342.922(477)
DOI https://doi.org/10.24144/2788-6018.2022.03.27

ЗАХИСТ ІНФОРМАЦІЇ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Баран М.В.,
здобувачка кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
https://orcid.org/0000-0002-2434-855X

Баран М.В. Захист інформації у контексті забезпечення інформаційної безпеки.

У статті на підставі чинного законодавства з позиції адаптації національної нормативно-правової бази до вимог Європейського Союзу розглянуто захист інформації у контексті забезпечення інформаційної безпеки. В основу методології наукового дослідження покладено факторний, причинно-наслідковий аналіз, спрямований на виявлення обставин для комплексного та системного дослідження характеру впливу захисту інформації на інформаційну безпеку. Актуальність дослідження зумовлена впливом розвитку інформаційно-комунікаційних технологій на захист інформації у контексті забезпечення інформаційної безпеки. Зазначено, що інформаційна безпека охоплює захист конфіденційності та забезпечення стану захищеності конституційних права і свободи людини та громадянина, передбачає можливість доступу та використання інформації, ставлячи питання про захист інформації. Захист інформації забезпечує цілісність, достовірність, точність та повноту інформації.

Нормативно-правове регулювання захисту інформації включає норми, які впорядковують суспільні відносини, що виникають у процесі інформаційної взаємодії між фізичними та юридичними особами та державою. Вказано, що розвиток цифрової економіки зумовили необхідність внесення поправок у правове регулювання захисту інформації, яке не встигає адекватно реагувати на зміни у технологічному та соціальному аспектах у соціумі. Підкреслено необхідність захисту комерційної та професійної таємниці, державної таємниці, інсайдерської інформації, персональних даних. На підставі аналізу реалізації захисту інформації щодо забезпечення конфіденційності стосовно інформації обмеженого доступу у контексті забезпечення інформаційної безпеки визначено ряд закономірностей, які враховані у визначенні тенденцій щодо захисту інформації. Зазначено, що захист інформації повинен бути нормативно закріплений щодо усіх видів інформації обмеженого доступу.

Ключові слова: інформація обмеженого доступу, доступ до інформації, конфіденційність, нормативно-правове регулювання, цифрова економіка.

Baran M.V. Information protection in the context of information security.

The article based on current legislation from the standpoint of adaptation of the national legal framework to the requirements of the European Union considers the protection of information in the context of information security. The methodology of scientific research based on factor, causal analysis, aimed at identifying the circumstances for a comprehensive and systematic study of the nature of the impact of information protection on information security. The relevance of the study is due to the impact of the development of information and communication technologies on information protection in the context of information security. It is noted that information security covers the protection of confidentiality and ensuring the state of protection of constitutional rights and freedoms of man and citizen, provides access to and use of information, raising questions about the protection of information. Information protection ensures the integrity, reliability, accuracy and completeness of information.

Regulatory and legal regulation of information protection includes norms that regulate public relations that arise in the process of information interaction between individuals and legal entities and the state. It pointed out that the development of the digital economy has necessitated amendments to the legal regulation of information protection, which does not have time to adequately respond to changes in technological and social aspects in society. The need to protect trade and professional secrets, state secrets, insider information, personal data is em-

phasized. Based on the analysis of the implementation of information protection to ensure the confidentiality of restricted information in the context of information security, a number of patterns are identified, which are taken into account in determining trends in information protection. It is stated that the protection of information should be regulated for all types of restricted information.

Key words: restricted access information, access to information, confidentiality, normative-legal regulation, digital economy.

Постановка проблеми. Розвиток цифрових технологій та зростання обороту цифрових даних у всіх сферах життя суспільства та управління, включаючи інформацію обмеженого доступу, що відповідає вимогам конфіденційності, обумовлює актуальність питання забезпечення інформаційної безпеки. Загрози безпеці в інформаційному середовищі існують для всіх видів інформації та інформаційних процесів. В останнє десятиліття ведуться активні дослідження можливості забезпечення конфіденційності інформації у мобільних мережах за рахунок механізмів мережевого рівня моделі взаємозв'язку відкритих систем. У цьому випадку користувачеві достатньо визначити свій профіль захисту інформації щодо кількісної чи якісної оцінки параметрів інформаційної безпеки. Водночас застосування новітніх технологій вимагає розроблення відповідного нормативно-правового регулювання.

Стан опрацювання проблематики. Важливе значення для розробки проблеми мали праці вчених-правознавців: І. В. Арістової, О. А. Баранова, К. І. Бєлякова, І. Р. Березовської, В. М. Брижка, В. М. Глушкова, Б. А. Кормича, Г. М. Линника, А. І. Марущака, А. М. Новицького, Н. Б. Новицької, О. В. Олійника, В. Ф. Опришка, В. Г. Пилипчука, І. М. Сопілко, М. Я. Швеця, В. С. Цимбалюка та ін. Зміни, що відбуваються в системі соціального регулювання, доповнюються метаморфозами, які супроводжують технічну регламентацію стосовно вимог до виробничих, технологічних, логістичних та інших процесів, у матеріальному базисі вимагають проведення теоретико-прикладних досліджень захисту інформації у контексті забезпечення інформаційної безпеки.

Метою статті є дослідження захисту інформації у сфері забезпечення інформаційної безпеки.

Виклад основного матеріалу. Досягнутий у даний час баланс у системі правових норм, які регулюють інформаційні відносини, у тому числі у сфері інформаційної безпеки та захисту інформації, не є абсолютним. Правові засоби завжди обмежені рівнем суспільного розвитку. Цілі, які визначаються законодавцем є ідеальними та за суттю не завжди узгоджуються з рівнем розвитку впровадження та використання інформаційних технологій. Це призводить до невідповідності у відносинах поставлених цілей та обраних для їх досягнення засобів. Активізація процесу законотворчості з регулювання правовідносин в інформаційній сфері значно ускладнена відсутністю стрункої системи регламентації правових відносин і розвитком цього сегмента законодавства [1].

Специфіку нормативно-правового регулювання відносин у сфері забезпечення інформаційної безпеки визначають дві обставини. Першою є невизначеність кордонів і змісту державних, суспільних та приватних інтересів в інформаційній сфері, що пояснюється широтою та багатоаспектністю останньої. Друга обставина пов'язана з об'єктивно зумовленою різницею динаміки правотворчого процесу та темпів технічного та технологічного розвитку у сфері інформаційної взаємодії. Така відмінність визначає існування непереборної неадекватності правового регулювання характеру суспільних зв'язків щодо засобів і способів отримання, накопичення, обробки, зберігання та передачі інформації. Ефективність юридичного впливу в даному випадку може бути досягнута, якщо орієнтувати застосовувані правові регулятори не на реальні, а на прогнозовані суспільні відносини у цій галузі.

Питання захисту інформації активно впливають на забезпечення інформаційної безпеки. Захист інформації стосовно питань інформаційної безпеки має безпосереднє відношення і виступає однією з імперативних умов. Є зворотний зв'язок між ними, оскільки порушення вимог інформаційної безпеки може створити загрозу не лише порушенню конфіденційності, але й цілісності та достовірності інформації.

Інформаційна безпека передбачає захист конфіденційності та забезпечення стану захищеності конституційних права і свободи людини та громадянина. Відповідно, забезпечення інформаційної безпеки передбачає можливість доступу та використання інформації.

Великі інформаційні потоки, що розповсюджуються, у тому числі з використанням технологій великих даних, складають величезний масив, робота з яким передбачає вживання заходів для захисту інформації та забезпечення до неї доступу. Важливою складовою цих заходів є організаційно-правові, технічні, програмно-апаратні та інші заходи інформаційної безпеки. Забезпечення захисту можна розглядати насамперед як складову частину стану захищеності.

Інформаційна безпека як стан захищеності передбачає низку станів, зокрема стан забезпечення та захисту права і свободи людини та громадянина. Останнє дозволяє повноцінно проводити заходи захисту інформації та за-

безпечити захист прав і свобод людини та громадянина в інформаційній сфері.

Забезпечення захисту інформації постає як одна з вимог її певного законного стану. До вимог включаються вимоги щодо цілісності, достовірності, точності та повноти інформації. Тільки за наявності сукупності цих вимог можна говорити про повноцінний захист інформації.

Відповідно до чинних вимог, до засобів забезпечення користування офіційними сайтами органів публічної адміністрації, з метою захисту інформації, розміщеної на офіційному сайті, має бути забезпечено: ведення електронних журналів обліку операцій, виконаних за допомогою програмного забезпечення та технологічних засобів ведення офіційного сайту, що дозволяють забезпечувати облік дій щодо розміщення, зміни та видалення інформації на офіційному сайті, фіксувати точний час, зміст змін та інформацію про уповноваженого співробітника органу виконавчої влади або оператора офіційного сайту, який здійснив зміни на офіційному сайті; щоденне копіювання інформації та електронних журналів обліку операцій на резервний матеріальний носій, що забезпечує можливість відновлення; захист інформації від знищення, модифікації та блокування доступу до неї, від неправомірних дій щодо інформації; зберігання резервних матеріальних носіїв із щоденними копіями; застосування шифрованих механізмів та сертифікатів безпеки при передачі даних, що забезпечують шифрування та захист інформації, що передається, у тому числі персональних даних користувачів офіційних сайтів [2]. Цей набір заходів дозволяє забезпечити захист інформації разом із цілісністю, точністю та повнотою.

Захист інформації має важливе значення для забезпечення конфіденційності інформації як стану, при якому відбувається захист інформації від несанкціонованого доступу третіх осіб. Конфіденційність сприймається як властивість інформації, що зумовлено забезпеченням інформаційної безпеки.

Правову властивість конфіденційності інформації слід визначати, як стан обмеження доступу до інформації, що охороняється, у тому числі щодо використання, розповсюдження та надання, встановлений законами є інтегративним результатом застосування організаційно-правових заходів у рамках спеціального правового режиму з метою забезпечення оборони країни та державної безпеки, інформаційної безпеки, охорони прав, свобод та законних інтересів різних суб'єктів.

Забезпечення захисту інформації доцільно розглядати як умову, що дозволяє говорити про конфіденційність інформації. Тому заходи, які вживаються задля забезпечення конфіденційності інформації, передбачають захист цієї інформації. У процесах забезпечення конфіденційності інформації обмеженого доступу має безпосередньо реалізовуватись захист інформації.

Нормативне регулювання захисту інформації у найзагальнішому сенсі включає зведення правил, які впорядковують відносини, що виникають у суспільстві щодо інформації між фізичними, юридичними особами та державою. Розвиток науково-технічного прогресу та експансія цифрової економіки зумовили необхідність внесення суттєвих поправок до правового регулювання, яке не встигає адекватно реагувати на зміни, що стрімко відбуваються в соціумі.

Ряд авторів розглядає вимогу щодо забезпечення захисту інформації як складову частину поряд з конфіденційністю при забезпеченні інформаційної безпеки стосовно певного виду інформації обмеженого доступу. Щодо професійної таємниці, фахівці висловлюють позицію, що суб'єкт професійної діяльності не тільки зобов'язаний забезпечувати конфіденційність відомостей, а й забезпечувати інформаційну безпеку професійної діяльності.

Надання довірителем відомостей, що становлять професійну таємницю, обумовлено наявністю довіри особистого характеру або пов'язаного з особливим професійним статусом суб'єкта професійної діяльності. Це передбачає, що обидві сторони правовідносин у сфері професійної таємниці розраховують на захист інформації, що отримується та зберігається.

У сфері комерційної таємниці, де витік інформації може призвести до значних майнових втрат, сторони, які використовують відповідну інформацію, повинні враховувати захист інформації. У зв'язку з цим в угодах про використання відомостей, що становлять комерційну таємницю, у договорах про передачу прав на секрети виробництва (ноу-хау) прямо передбачається вимога забезпечення захисту інформації. Власник або правовласник такої інформації повинен передавати третім особам лише необхідну інформацію, останні зобов'язані повідомляти про використання комерційно цінної інформації.

Судова практика підтверджує, що стосовно комерційної таємниці пред'являються вимоги захисту інформації, а також вимоги про належність інформації до комерційної таємниці.

З усіх видів інформації обмеженого доступу для інсайдерської інформації встановлюється вимога про заборону використання [3]. Інсайдерська інформація – це інформація, яка не була поширена, в тому числі відомості, що становлять комерційну, службову, банківську таємницю, іншу таємницю, що охороняється законом, поширення якої може мати істотний вплив на ціни фінансових інструментів, іноземної валюти та товарів, у тому числі відомості, що стосуються одного або кількох емітентів емісійних цінних

паперів, однієї або кількох управляючих компаній інвестиційних фондів, пайових інвестиційних фондів та недержавних пенсійних фондів або одного або кількох фінансових інструментів, іноземної валюти та товарів [4, с. 177].

Забезпечення захисту інформації прямо випливає із вимоги забезпечення конфіденційності відомостей, що належать до державної таємниці. В Законі України «Про державну таємницю» зазначено, що віднесення відомостей до державної таємниці та їх засекречення здійснюється відповідно до принципів законності, обґрунтованості та своєчасності [5]. Забезпечення обґрунтованості передбачає проведення експертної оцінки відомостей щодо доцільності засекречування чи розсекречення. Доцільність віднесення засекречування недостовірної інформації навряд чи обґрунтовано.

Закон України «Про інформацію» щодо законності передбачає дотримання вимог інформаційного законодавства та реалізацію захисту інформації [6].

Вимога забезпечення захисту інформації прямо встановлена щодо кредитних історій. Зокрема, ст. 4 Закону України «Про організацію формування та обігу кредитних історій» закріплює, що принципами формування та доступу до інформації, яка складає кредитну історію, є: конфіденційність інформації та її захист [7]. Закон покладає на джерело формування кредитної історії обов'язок щодо повідомлення достовірної інформації та необхідності її оновлення.

Відповідно до Закону України «Про захист персональних даних», при обробці персональних даних повинні бути забезпечено захист персональних даних, їх достатність, а в необхідних випадках актуальність стосовно мети обробки персональних даних [8]. Оператор повинен вживати необхідних заходів або забезпечувати їх прийняття щодо видалення чи уточнення неповних, або точності та актуальності інформації.

Аналіз законодавства про персональні дані свідчить, що більшість підзаконних нормативно-правових актів у цій сфері фактично дублює вимогу щодо захисту, але не розкриває заходи направлені на захист інформації. Закон України «Про захист персональних даних» покладає на оператора персональних даних обов'язок захисту, надання точної інформації та обов'язковість її актуалізації, оновлення при настанні відповідних обставин і передачі відповідних даних.

Однак сьогодні кількість згод, які видає суб'єкт персональних даних, перевищує всі можливості людини реально відстежувати всіх операторів, кому надано такі дані. Виникає питання необхідності створення автоматизованих систем, за допомогою яких суб'єкт персональних даних міг би контролювати операторів, які обробляють його дані та через ці системи міг би оновлювати свої дані. Для операторів це значно збільшить роботу з обробки даних і створить ризики витоку великих обсягів даних. У зв'язку з чим варто розглянути питання про зміну обов'язку суб'єкта захисту так, як даний аспект безпосередньо зв'язний з розвитком цифрової економіки.

Питання формування єдиного інформаційного простору цифрової економіки України багато в чому дискусійне з технологічної точки зору, має ряд теоретичних, практичних і організаційних задач національного та міжнародного рівня, що у деякій мірі враховано у Національній економічній стратегії на період до 2030 року [9, с. 2028; 10].

Аналіз реалізації захисту інформації у відносинах, пов'язаних із забезпеченням конфіденційності стосовно інформації обмеженого доступу у контексті забезпечення інформаційної безпеки, свідчить про низку закономірностей:

- законодавець у цій сфері поки що не використовує активно прямі вимоги щодо забезпечення захисту інформації, частіше використовуючи вимоги щодо забезпечення точності, достатності, цілісності, незмінності інформації;

- захист інформації є однією з умов наявності конфіденційності та достатності заходів щодо її забезпечення, ця вимога повинна відображатися у нормативних вимогах опису заходів захисту конфіденційності стосовно всіх видів інформації обмеженого доступу;

- захист інформації повинен знайти закріплення в інституційних засадах усіх видів інформації обмеженого доступу та повинен знайти відображення у нормах відповідних законів, які встановлюють режими різних видів інформації, доступ до якої обмежений.

Важливо розвивати забезпечення достовірності з позиції захисту від поширення хибної інформації та іншої дезінформації як серйозної інформаційної загрози не лише на національному, а й на міжнародному рівні. Про необхідність реалізації державної політики у сфері протидії створенню та розповсюдженню дезінформації та іншої недостовірної інформації свідчить низка важливих документів. Поширення недостовірної інформації сприймається як загроза інформаційній безпеці. Держави Європейського Союзу розглядають поширення дезінформації, у тому числі фейкової інформації, як правопорушення.

Серед ключових тенденцій у сфері правових заходів інформаційної безпеки у контексті забезпечення інформаційної безпеки фахівці виділяють:

- активний розвиток стратегічних документів, спеціальних нормативно-правових актів щодо захисту інформації, зокрема удосконалення Закону України «Про захист інформації в інформаційно-комунікаційних системах» [11];

- закріплення на державному рівні системи засобів забезпечення захисту інформації, розробка планів щодо реалізації системи;

- реалізація директивних документів Європейського Союзу щодо критеріїв забезпечення захисту інформації;

- системний підхід до обмежень і заборон в інформаційному просторі, удосконалення структури органів, які здійснюють контроль і нагляд у цій сфері;

- розвиток державних програм з навчання щодо захисту інформації; удосконалення системи юридичної відповідальності у сфері інформаційної безпеки;

- використання технологій штучного інтелекту у протидії загрозам безпеці інформації; вживання комплексу спеціальних заходів щодо протидії поширенню фейкової інформації.

Аналіз стану правового регулювання захисту інформації у контексті забезпечення інформаційної безпеки дає змогу говорити, що розвиток правових засобів захисту інформації в Україні відстає від технічних, організаційних, програмно-апаратних та інших. Відсутнє спеціальне регулювання з цього питання, не сформовано єдиний понятійний апарат, принципи правового забезпечення захисту інформації у контексті інформаційної безпеки не сформульовано на державному рівні; неефективно застосовується система правових заборон та обмежень в інформаційному просторі, не розвивається система мережевого державного суверенітету.

Більшість правових засобів, що приймаються, пов'язані з окремими інститутами – забезпечення захисту інформації обмеженого доступу, в тому числі державної таємниці, комерційної таємниці, персональних даних; інституту критичної інфраструктури; протидії злочинам у сфері комп'ютерної інформації та ін. Серед основних завдань адміністративно-правового регулювання щодо інформації, інформаційно-інфраструктурних відносин, об'єктом яких виступають засоби зв'язку, інформатизації та захист інформації і інформаційна безпека, можна виділити контроль за інформаційними потоками, забезпечення інформаційної безпеки (в інформаційному та технічному аспектах) [12, с. 28].

У Стратегії національної безпеки України встановлено, що забезпечення інформаційної безпеки здійснюється шляхом реалізації державної політики, спрямованої на вирішення завдань щодо формування безпечного середовища обігу інформації, доведення до громадськості достовірної інформації [13].

Стратегія інформаційної безпеки України як документ стратегічного планування закріплює аналогічне положення, встановлюється, що реалізація національних інтересів в інформаційній сфері спрямована на формування безпечного середовища обігу інформації та стійкого до різних видів впливу інформаційної інфраструктури з метою забезпечення конституційних прав і свобод людини та громадянина, стабільного соціально-економічного розвитку країни, національної безпеки України [14].

Висновки. Цінність інформації щодо цифрової економіки набуває нового значення. Підходи до інформаційного менеджменту не так сприяють формуванню доданої вартості процесів захисту інформації, як створюють потенціал для отримання додаткової цінності інформації. Реалізація захисту інформації щодо забезпечення конфіденційності здійснюється переважно з використанням законодавчих вимог забезпечення не захисту, а інших вимог, що пред'являються законодавчо. Нормативно-правове забезпечення режиму захисту інформації обмеженого доступу розвивається шляхом включення вимог щодо забезпечення достовірності, точності і інших критеріїв інформації. Захист інформації має знайти закріплення у системі інституційних принципів всіх видів інформації обмеженого доступу.

Ефективність правового регулювання захисту інформації у контексті забезпечення інформаційної безпеки проявляється у вдосконаленні законотворчої діяльності, що створює затребувані часом норми права, в яких знаходять відображення інтереси та потреби членів соціуму та присутній адміністративний ресурс силових структур держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Малашко О. Є., Єсімов С. С. Нормативно-правове забезпечення інформаційної безпеки в Україні. Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки. 2020. № 14 (94). Т. 2. С. 30–38.
2. Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади: Постанова Кабінету Міністрів України від 12.06.2019 р. № 493. URL. https://zakon.rada.gov.ua/laws/show/493-2019-%D0%BF#Text.
3. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006 р. № 3480-IV. URL. https://zakon.rada.gov.ua/laws/show/3480-15#Text.
4. Шевченко С. М., Жданова Ю. Д., Складанний П. М., Бойко С. В. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Кібербезпека. 2022. № 3 (15). С. 175–185.
5. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. URL. https://zakon.rada.gov.ua/laws/card/3855-12.
6. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL. https://zakon.rada.gov.ua/laws/card/2657-12.

7. Про організацію формування та обігу кредитних історій: Закон України від 23.06.2005 р. № 2704-IV. URL. https://zakon.rada.gov.ua/laws/card/2704-15.
8. Про захист персональних даних: Закон України від 01.06.2010 р. № 2704-VI. URL. https://zakon.rada.gov.ua/laws/show/2297-17#Text.
9. Сопільник Л., Ковалів М., Єсімов С., Скриньковський Р. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. Traektoriâ Nauki = Path of Science. 2020. Vol. 6. № 5. S. 2023-2032.
10. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text.
11. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL. https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80.
12. Єсімов С. С. Використання інформаційних технологій як предмет адміністративно-правового регулювання. Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки. 2015. № 827. С. 24–29.
13. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL. https://zakon.rada.gov.ua/laws/show/ 392/2020#Text.
14. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL. https://zakon.rada.gov.ua/laws/show/685/2021#Text.