УДК 342.817:351.746.1
DOI https://doi.org/10.24144/2788-6018.2022.04.43

СИСТЕМА ПРАВОВИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ярема О.Г.,
кандидат юридичних наук,
доцентка, доцентка кафедри
адміністративно-правих дисциплін
Львівського державного університету внутрішніх справ
https://orcid.org/0000-0003-3550-0454

Ілюшик О.М.,
кандидат юридичних наук,
доцентка, доцентка кафедри
адміністративно-правих дисциплін
Львівського державного університету внутрішніх справ
https://orcid.org/0000-0003-3451-0887

Ярема О.Г., Ілюшик О.М. Система правових засобів забезпечення інформаційної безпеки.

Стаття присвячена висвітленню актуальної проблеми інформаційного права – питання системи правових засобів забезпечення інформаційної безпеки. Розглядаються засоби забезпечення інформаційної безпеки – правові, організаційні та технічні. Висвітлюються основні теоретичні положення щодо правових, організаційних і технічних засобів у контексті інформаційної безпеки, проводиться оцінка проблем у досліджуваній галузі. Правова природа загальних правових засобів забезпечення інформаційної безпеки базується на: законодавчому закріпленню понятійного апарату щодо інформаційної безпеки; формуванні системи правового забезпечення інформаційної безпеки. Інформаційна безпека у зазначеному аспекті розглядається, як об'єкт правової охорони, щодо захищеності законних прав і інтересів особи, суспільства та держави від деструктивного інформаційного впливу та захисту інформації від незаконних перетворень. Серед засобів забезпечення інформаційної безпеки виділено: форми чи способи фіксації інформації; офіційне електронне оприлюднення, зокрема опублікування, використання систем розподілених реєстрів, зокрема технологій блокчейн; проведення перевірок інформації у контексті інформаційної безпеки; презумпція безпеки інформації щодо інформаційної безпеки. Зазначене дозволяє конкретизувати напрями правового регулювання у сфері інформаційної безпеки. Одним з правових засобів забезпечення інформаційної безпеки є юридична відповідальність, яка передбачена кримінальним, адміністративним, цивільно-правовим, трудовим законодавством. Указано, що для забезпечення інформаційної безпеки використовуються юридичні прийоми: встановлення права на достовірну інформацію; затвердження обов'язкової форми або способу фіксації інформації як засобу забезпечення інформаційної безпеки; реалізація публічного визнання; здійснення моніторингу та перевірки інформації у контексті інформаційної безпеки; застосування презумпції захисту інформації щодо інформаційної безпеки; встановлення юридичної відповідальності.

Ключові слова: інформація, захист інформації, правове регулювання, презумпція безпеки інформації, юридична відповідальність.

Yarema O.G., Ilyushyk O.M. System of legal remedies for ensuring information security.

The article is devoted to highlighting the current problem of information law, the issue of the system of legal means of ensuring information security. The means of ensuring information security are considered - legal, organizational and technical. The main theoretical provisions regarding legal, organizational and technical means in the context of information security are highlighted; the problems in the researched field are assessed. The legal nature of general legal means of ensuring information security is based on: legislative consolidation of the conceptual apparatus regarding information security; formation of the system of legal support of information security. Information security in the specified aspect is considered as an object of legal protection, regarding the protection of legal rights and interests of the person, society and the state from destructive informational influence and protection of information from illegal transformations. Among the means of ensuring information security, the following are highlighted: forms or methods of recording information; official electronic publication, in particular publication, use of distributed ledger systems, in particular block chain technologies; conducting checks of information in the context of information security; presumption of information security regarding information security. This

allows us to specify the directions of legal regulation in the field of information security. One of the legal means of ensuring information security is legal liability, which is provided for by criminal, administrative, civil law, and labor legislation. It is indicated that legal techniques are used to ensure information security: establishment of the right to reliable information; approval of a mandatory form or method of recording information as a means of ensuring information security; implementation of public recognition; monitoring and verification of information in the context of information security; application of the presumption of information protection regarding information security; establishment of legal responsibility.

Keywords: information, information protection, legal regulation, presumption of information security, legal responsibility.

Постановка проблеми. Розвиток інформаційного суспільства та перехід до суспільства знань нерозривно пов'язані з посиленням значення інформації. Поширення фейкової інформації, необхідність повторної перевірки практично будь-якої інформації, що циркулює через засоби масової комунікації, детермінують осмислення проблем достовірності інформації вже на якісно іншому рівні з метою забезпечення інформаційної безпеки, виділеної як пріоритетне спрямування державної політики України та визначеної Стратегією інформаційної безпеки, спрямованої на формування безпечного середовища обігу інформації та надання її громадськості. Вимагає уваги питання забезпечення інформаційної безпеки, здійснюваного за допомогою законодавчого закріплення низки засобів, завдяки яким держава публічно визнає та гарантує інформаційну безпеку.

У такому контексті актуальними видаються наступні напрями досліджень інформаційного права: закріплення національних інтересів України в інформаційній сфері у нормативно-правових актах; правові засади забезпечення інформаційної безпеки держави, суспільства та особи; правові механізми забезпечення інформаційної безпеки; теоретико-правові засади протидії загрозам інформаційній безпеці України; теоретичні і правові основи захисту інформаційного простору України; теоретичні і правові основи захисту інформаційних ресурсів України; компетенція державних органів України, зокрема правоохоронних, щодо забезпечення інформаційної безпеки України; взаємодія державних органів України в процесі забезпечення інформаційної безпеки держави; теоретико-правові основи оцінювання протиправних дій учасників інформаційно-психологічного протиборства; теоретико-правові основи використання комунікаційних каналів з метою здійснення інформаційного впливу; міжнародний досвід діяльності державних органів із забезпечення інформаційної безпеки тощо [1, с. 25-26].

Окремі проблеми цієї тематики досліджуються в працях: О.В. Арістової, О.А. Баранова, К.І. Бєлякова, В.М. Брижка, С.С. Єсімова, Р.А. Калюжного, М.В. Коваліва, О.В. Копана, В.К. Конаха, Б.А. Кормича, О.В. Коржа, О.В. Кохановської, О.В. Марущака, В.Г. Пилипчука, Н.А. Савінової, І.М. Шопіної, М.Я. Швеця і інших.

Метою статті є дослідження системи правових засобів забезпечення інформаційної безпеки, виявлення тенденції формування в законодавстві України презумпції інформаційної безпеки.

Виклад основного матеріалу. Критерії інформаційної безпеки стають все складнішими, тому важливо не просто вживати окремих заходів забезпечення безпеки, а й вибудовувати цілісну систему засобів, що включає низку інструментів, прийомів, якими міг би скористатися законодавець або особа, яка застосовує права для забезпечення інформаційної безпеки за різних суспільних відносин. Засоби забезпечення безпеки можна розмежувати на правові, організаційні, технічні та інші. Правові засоби – сукупність прийомів, способів, які закріплені у нормах права задля забезпечення інформаційної безпеки. Організаційні засоби – це сукупність прийомів, способів організаційного характеру, що дозволяють забезпечити інформаційну безпеку у суспільних відносинах. Технічні та програмно-апаратні засоби представляють сукупність прийомів, засобів забезпечення інформаційної безпеки за допомогою використання відповідних засобів, програм для електронно-обчислювальних машин, програмно-апаратних засобів. Як наприклад, може виступати електронний підпис. Інформаційна безпека встановлюється не лише на рівні нормативно-правових актів, а й рядом технічних норм. У такий спосіб відбувається встановлення технічних засобів інформаційної безпеки.

Загальні правові засоби забезпечення інформаційної безпеки включають: законодавче закріплення понятійного апарату у сфері забезпечення інформаційної безпеки; формування системи правового забезпечення інформаційної безпеки; законодавче закріплення інформаційної безпеки, основних ідей, положень, що відображають особливості: системи заборон, зобов'язань, дозволів, стимулів, обмежень, інших правових засобів забезпечення інформаційної безпеки. Система конкретних юридичних прийомів, що використовуються для забезпечення інформаційної безпеки, включає прийоми та засоби, представляє певну їх сукупність.

Інформаційна безпека в інформаційному суспільстві набуває важливого стратегічного значення. При активному впровадженні та використанні цифрових технологій, зокрема штучного інтелекту та платформних рішень, з'являється більше ризиків, що зумовлюють поширення значних обсягів інформації недостовірного характеру. Ідея права на достовірну інформацію безпо-

середньо випливає із необхідності забезпечення інформаційної безпеки. Це проявляється у сукупності правових можливостей, які закріплюються за суб'єктами права – фізичними і юридичними особами, публічними утвореннями. Ряд спеціальних суб'єктів наділяється даним правом. Особливе значення має забезпечення даного права для фізичних осіб.

Серед прав, що включаються до суб'єктивного права на захист інформації, є можливим виділити такі права: право вимоги оновлення інформації, надання достовірної інформації, уточнення інформації, виправлення інформації у разі її модифікації, відновлення; можливості використання достовірної інформації тощо. Вони є складовими елементами права на захист інформації стосовно різних її проявів.

Встановлення пріоритетної форми чи способу фіксації інформації доцільно розглядати як забезпечення інформаційної безпеки. Даний засіб передбачає закріплення законодавцем форм і способів фіксації інформації.

Законодавець встановлює, що при виникненні сумнівів і суперечок пріоритет надається певній формі чи способу фіксації інформації. Визнання захищеної інформації може здійснюватися з допомогою офіційного електронного оприлюднення, зокрема опублікування. Особливого значення цей спосіб визнання має щодо правової інформації. Пріоритет мають офіційні джерела правової інформації під час роботи з нею. Таким пріоритетним способом фіксації інформації є публічні реєстри інформації, офіційні банки та бази даних [2]. Офіційний, обов'язковий чи інший спосіб закріплення пріоритетності певних форм та способів фіксації інформації відіграє важливу роль у забезпеченні інформаційної безпеки.

Одним із правових засобів забезпечення інформаційної безпеки є публічне визнання. Таке визнання можливе на основі необхідності виконання нормативно встановлених вимог про публічне визнання створеної інформації, що надається або розповсюджується. Публічна заява може бути здійснена на основі вимог, встановлених договором, через пряме волевиявлення суб'єктів як гарантія забезпечення безпеки.

Визнання безпеки в законодавстві здійснюється у різних формах: заяв, що подаються на вчинення юридично значущих дій; визнання інформаційної безпеки через подальше поширення інформації як безпечної; визнання безпеки через підписання угоди та оприлюднення даних про цей факт (характерно для приватноправових відносин); спеціальних свідоцтв про інформаційну безпеку в відомостях, що надаються.

У разі цифровізації однією з форм визнання інформаційної безпеки є використання систем розподілених реєстрів, зокрема технологій блокчейн (англ. Blockchain). Однією з ключових вимог до таких систем є незмінність інформації, що знаходиться на платформі блокчейн, або неможливість зміни без відображення цього факту в системі [3]. Будь-які операції з інформацією та її зміна призводять до фіксації цього факту, вони стають доступними для всіх користувачів платформи. За рахунок публічного відображення всіх змін інформації встановлюється важлива гарантія забезпечення захисту. Відбувається публічне визнання інформаційної безпеки. Такі форми визнання безпеки є перспективними та розвиваються на рівні окремих бізнес-процесів, у сфері публічного управління, де дуже важливо забезпечити довіру до цифрового середовища та використовуваних органами влади технологій.

Одним із засобів забезпечення інформаційної безпеки є проведення відповідних перевірок. Перевірка інформаційної безпеки здійснюється у межах надання адміністративних послуг [4].

Міністерство юстиції України під час ведення державного реєстру громадських об'єднань здійснює перевірку повноти інформації, що міститься у поданих документах [5]. У правовому регулюванні очевидна тенденція закріплення перевірки інформації стосовно всіх офіційних потоків інформації, що мають публічне значення.

Перевірка безпеки здійснюється за допомогою запиту додаткових відомостей, уточнюючих відомостей, додаткових документів, що підтверджують достовірність інформації. Можуть бути використані такі інструменти, як звернення та запити відповідно до встановленого законодавством порядку. Можуть встановлюватись спеціальний термін та вимоги до змісту відповіді на запити.

Перевірка інформаційної безпеки може здійснюватися суб'єктами, які беруть участь в інформаційних процесах, зовнішніми незалежними суб'єктами. Наприклад, у межах аудиторської перевірки з використанням організаційних заходів, що застосовуються безпосередньо, наприклад, здійснення зіставлення, порівняння, аналізу та інших методів і способів, з використанням технічних та програмно-апаратних засобів.

Активно використовуються технології штучного інтелекту, що дозволяють здійснити перевірку та встановити недостовірну інформацію на рівні окремих повідомлень, відео файлів, акаунтів у мережі Інтернет та окремих сайтів в Інтернеті [6, с. 11].

Перевірка безпеки розглядається переважно як окрема процедура у складі інформаційних процесів і адміністративних процедур, але може бути самостійною адміністративною процедурою. Державі необхідно розробити систему прийомів, способів, за допомогою яких реалізовуватиметься самостійна адміністративна процедура.

У законодавстві формується тенденція до презумпції інформаційної безпеки. Це один із

правових засобів, що дозволяють забезпечувати інформаційну безпеку, захищати права і законні інтереси власників інформації.

Презумпція безпеки передбачає, що власник інформації у разі надання або розповсюдження третім особам отримує гарантію, що йому не доведеться вчиняти додаткові дії доведення та обґрунтування факту безпеки. Відбувається спрощення обігу інформації, скорочуються витрати на окремі операції, події з інформацією [7, с. 7008]. Для користувача інформації, який отримує від власника або іншого користувача інформації, зокрема оператора, інформацію, з'являється гарантія, що використовує достовірну інформацію.

Презумпція інформаційної безпеки або усвідомленої добровільності означає, що інформація визнається безпечною, допоки зворотне не буде доведено рішенням суду [8, с. 131]. Ця презумпція виконує кілька важливих функцій: забезпечує законність дій з інформацією (оскільки така презумпція встановлюється на рівні закону, який дозволяє визнавати інформацію достовірною, доки зворотне не буде встановлено судом); гарантує факт інформаційної безпеки (можна говорити про гарантію за умови, що має безстроковий характер, доки інформація зберігає актуальність, значущість, не застаріла через об'єктивні фактори); правозахисну функцію, оскільки презумпція дозволяє захистити права та законні інтереси учасників інформаційних правовідносин, забезпечених цією презумпцією; оцінна та аксіологічна функції, що дозволяють оцінити значущість та цінність інформації для суб'єктів інформаційних процесів.

Фактично користувачі інформації, щодо якої встановлюється презумпція інформаційної безпеки, оцінюють значимість і цінність інформації, що надається законом або договором. Суб'єкти значно вище оцінюють інформацію, що охороняється презумпцією безпеки у контексті законного або договірного режиму, ніж інформації, що не охороняється.

У другому випадку власнику або користувачу інформації у разі надання чи розповсюдження необхідно вдаватися до додаткових способів забезпечення інформаційної безпеки, що може вимагати значно більших фінансових, технічних, організаційних і інших витрат; превентивна функція, що дозволяє запобігти можливим порушенням у сфері інформаційної безпеки.

Презумпція інформаційної безпеки встановлюється переважно на рівні закону, оскільки становить особливий прояв обмеження права на інформацію. Користувач визнає інформацію захищеною, доки зворотне не буде доведено рішенням суду, що набрало законної сили.

Користувач інформації повинен реалізовувати правову можливість права на інформацію, у тому числі використання та розповсюдження інформації як достовірної. Він не може встановлювати заборони на дії з інформацією через її небезпеку. Таке правило не завжди виявляється вільним від можливих зловживань правом з боку правовласника чи користувача, який реалізує презумпцію інформаційної безпеки. Однак такі порушення не виключають можливості звернення користувача за відшкодуванням шкоди, заподіяної внаслідок використання недостовірної інформації.

Презумпція інформаційної безпеки може встановлюватися з договору виходячи з принципу свободи договору. Сторони, укладаючи певний договір, можуть встановити, що інформація, яка передається, визнається достовірною, доки зворотне не буде доведено законним рішенням суду.

Сторони можуть встановити визнання інформаційної безпеки стосовно певних визнаних достовірними способами та формами передачі або зберігання інформації. Такий підхід повністю відповідає положенням Закону «Про захист інформацію в інформаційно-комунікаційних системах» про те, що вона може бути об'єктом публічних, цивільних і інших правових відносин [9]. Презумпція як правовий засіб забезпечення інформаційної безпеки є важливим елементом механізму реалізації.

У системі правових засобів забезпечення інформаційної безпеки важливу роль відіграють система заборон, зобов'язань забезпечувати інформаційну безпеку та використання обмежень. Велике значення має застосування засобів стимулювання інформаційної безпеки.

Важливим правовим засобом забезпечення інформаційної безпеки є інститут юридичної відповідальності [10, с. 141]. За створення, використання чи розповсюдження недостовірної інформації встановлюється кримінальна, адміністративна, цивільно-правова, дисциплінарна та матеріальна відповідальність.

Дисциплінарна відповідальність може настати щодо працівника, якщо роботодавець на рівні локального правового акта передбачив вимоги інформаційної безпеки та можливості застосування заходів дисциплінарного характеру за порушення цих вимог. Наприклад, поширення недостовірної інформації у процесі здійснення трудової функції контрагентом, надання недостовірної інформації роботодавцю, що спричинило заподіяння негативних наслідків. У деяких випадках це може заподіяти матеріальні збитки роботодавцю, що може бути підставою матеріальної відповідальності працівника.

Поширення недостовірної інформації її окремих різновидів тягне кримінальну відповідальність. Збільшення кількості складів злочинів, пов'язаних з безпекою інформації у період воєнного стану свідчить про те, що кримінальна політика України націлена на визнання дій, пов'язаних з інформацією, у низці випадків як суспільно небезпечних, спрямована на криміналізацію та забезпечення захисту національних інтересів.

Адміністративна відповідальність розвивається у сфері дій, пов'язаних з інформаційною безпекою. Серед адміністративних правопорушень, передбачених Кодексом України про адміністративні правопорушення, можна виділити такі групи відповідальності: за надання недостовірних звітів; за відмову в наданні інформації; за надання недостовірних відомостей та ін.

За дії, пов'язані з недостовірною інформацією, настає цивільно-правова відповідальність відповідно до Цивільного кодексу України за поширення відомостей, що не відповідають дійсності; надання або розповсюдження недостовірної інформації, що спричинила збитки у межах договірних відносин; вчинення вищезгаданих правопорушень, що спричинили майнові збитки, вчинення інших протиправних дій, пов'язаних з недостовірною інформацією, що спричинили майнові збитки.

Підвищення значущості доступу до достовірної інформації вимагає переходу до концептуальної моделі доступу до інформації на основі безпечної інформаційної взаємодії суб'єктів з метою забезпечення національних інтересів. Для цього важливо розробити та законодавчо закріпити систему правових засобів, включаючи суб'єктивні права, гарантії, юридичну відповідальність, які забезпечують інформаційну безпеку.

Важливо на законодавчому рівні передбачити механізми забезпечення презумпції безпеки інформації щодо інформаційної безпеки у низці суспільних відносин для забезпечення стабільного інформаційного обміну та взаємодії. Можна виділити модель реалізації інформаційно-правового забезпечення інформаційної безпеки, що передбачає використання сукупності правових і інших засобів, вкладених у забезпечення інформаційної безпеки в інформаційних правовідносинах. Такі засоби поділяються на дві групи: загальні засоби, які застосовуються до більшості відносин, пов'язаних із забезпеченням інформаційної безпеки, спеціальні засоби, що використовуються для забезпечення безпеки стосовно конкретних відносин.

Висновки. Проведене дослідження дозволило довести, що для забезпечення інформаційної безпеки використовуються конкретні юридичні прийоми, до яких належать: встановлення права на достовірну інформацію; затвердження обов'язкової форми або способу фіксації інформації як засобу забезпечення безпеки; реалізація публічного визнання; здійснення моніторингу та перевірки інформаційної безпеки; застосування презумпції захисту інформації щодо інформаційної безпеки; встановлення юридичної відповідальності.

У ході дослідження виявлено тенденцію формування в законодавстві України презумпції інформаційної безпеки, яка передбачає, що власник інформації у разі надання чи розповсюдження третім особам отримує гарантію, що йому не доведеться вчиняти додаткові дії щодо доведення та обґрунтування факту інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Єсімов С.С. Використання інформаційних технологій як предмет адміністративно-правового регулювання. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2015. № 827. С. 24–29.
2. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL. https://zakon.rada.gov.ua/laws/card/1907-20.
3. Гурова А., Кірпачова М. Правові засади застосування блокчейну в космічній діяльності: особливості регулювання технології на національному, регіональному та міжнародному рівнях. *Підприємництво, господарство і право*. 2021. № 1. С. 265–275.
4. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15.07.2021 р. № 1689-IX. URL. https://zakon.rada.gov.ua/ laws/card/1689-20.
5. Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань: Закон України від 15.05.2003 р. № 755-IV. URL. https://zakon.rada.gov.ua/laws/card/755-15.
6. Ковалів М.В., Єсімов С.С., Кравчук С.М. Теоретичні засади правового регулювання систем штучного інтелекту щодо ідентифікації особи у контексті діяльності органів виконавчої влади. *Соціально-правові студії*. 2020. Випуск 2 (8). С. 8–15.
7. Єсімов С., Ковалів М., Скриньковський Р. Правові режими службової інформації в Україні (Legal Regimes of Official Information in Ukraine). *Traektoriâ Nauki = Path of Science.* 2018. Vol. 4. № 4. S. 7001–7012.
8. Принципи правового регулювання інституту інформаційної безпеки. *Науковий Вісник Ужгородського Національного Університету. Серія: право*. 2021. Том 66. С. 129–134.
9. Про захист інформацію 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
10. Арістова І.В., Баранов О.А., Дзьобань О.П. та ін.; Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / За заг. ред. К. І. Бєлякова. Київ: КВІЦ, 2019. 344 с.
11. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 10.05.2018 р. № 357. URL. https://zakon.rada.gov.ua/laws/show/357-2018-%D0%BF#Text.