УДК 342.6:342.922(477)
DOI https://doi.org/10.32782/2524-0374/2021-4/71

ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ В УКРАЇНІ

LEGAL ISSUES OF PROVIDING INFORMATION SECURITY IN UKRAINE

Шабетя С.А., провідний науковий співробітник
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

Несін В.В., провідний науковий співробітник
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

У статті проаналізовано правові питання забезпечення інформаційної безпеки особи в Україні. Встановлено, що забезпечення інформаційної безпеки особи в Україні має нерозривний зв'язок із інформаційним законодавством. Інформаційне законодавство та законодавство щодо інформаційної безпеки особи є відносно новою галуззю законодавства України й наразі перебуває тільки на етапі становлення. У цьому аспекті найбільш прийнятним варіантом його розвитку, на наш погляд, є розробка єдиного консолідованого нормативного акта, який визначить понятійний апарат; основні напрями державної політики забезпечення інформаційної безпеки особи, суспільства та держави; об'єкти інформаційної безпеки; суб'єктів, на яких покладається обов'язок її забезпечення; основні загрози інформаційній безпеці та способи протидії тощо. Під час проведеного дослідження було визначено, що правові питання забезпечення інформаційної безпеки особи безпосередньо пов'язані із визначенням загроз інформаційній безпеці особи і правових шляхів їх подолання. Першою загрозою є правовий вакуум у більшості питань забезпечення інформаційної безпеки особи, тобто відсутність єдиного нормативного акта, який би регламентував поняття інформаційної безпеки, її основні ознаки, засоби захисту, суб'єктів, на яких покладається обов'язок здійснювати захист тощо. Способом протидії зазначеній загрозі, на наш погляд, є прийняття Кодексу України «Про інформацію». Другою загрозою є порушення законодавства з питань інформаційної безпеки, зокрема порушення норм Кримінального кодексу України, Кодексу України про адміністративні правопорушення тощо. Способом протидії зазначеним загрозам має стати негайне звернення із заявою або повідомленням про кримінальне / адміністративне правопорушення до органів Національної поліції. Третьою загрозою є технічні помилки інформаційних систем (засобів), а також природні процеси, що впливають на передачу, прийом і зберігання інформації. Способом протидії в цьому випадку може бути використання перевіреної техніки, заборона її використання сторонніми особами, очікування налагодження систем передачі інформації її володільцями. Четвертою загрозою є зовнішні чинники. Подолати таку загрозу можна через захист українського суспільства від агресивного інформаційного впливу, розвиток публічної дипломатії тощо.

Ключові слова: інформаційна безпека, правове забезпечення, безпека особи, інформація, інформатизація.

The article analyzes the legal issues of information security of a person in Ukraine. It is established that ensuring information security of a person in Ukraine is inextricably linked with information legislation. Information legislation and legislation on personal information security is a relatively new branch of Ukrainian legislation and is currently only in its infancy. In this aspect, the most acceptable option for its development, in our opinion, is the development of a single consolidated normative act, which will define the conceptual apparatus; main directions of the state policy of ensuring information security of the person, society and the state; information security facilities; entities responsible for its provision; main threats to information security and methods of counteraction, etc. The study found that the legal issues of information security of the person are directly related to the identification of threats to information security of the person and the legal ways to overcome them. The first threat is the legal vacuum in most issues of information security of the person, the lack of a single regulation that would regulate the concept of information security, its main features, means of protection, entities responsible for protection, and so on. In our opinion, the adoption of the Code of Ukraine On Information is a way to counteract this threat. The second threat is the violation of information security legislation, in particular, the violation of the Criminal Code of Ukraine, the Code of Ukraine on Administrative Offenses, etc. The way to counteract these threats should be to immediately apply to the National Police with a statement or notification of a criminal / administrative offense. The third threat is technical errors of information systems (tools), as well as natural processes that affect the transmission, reception and storage of information. The method of counteraction in this case may be the use of proven equipment, the prohibition of third parties to use it, waiting for the establishment of information transmission systems by its owners. The fourth threat is external factors. Such a threat can be overcome through the protection of Ukrainian society from aggressive information influence, the development of public diplomacy, and so on.

Key words: information security, legal support, personal security, information, informatization.

Вступ. В умовах глобалізації відбуваються постійні процеси зближення інформаційних систем окремих країн і формування на їхній основі єдиного інформаційного простору, впровадження інформаційних технологій у всі сфери життя особи. Глобальний процес інформатизації охопив усі сучасні країни світу. У таких умовах забезпечення інформаційної безпеки особи стає одним із найважливіших напрямів державної політики. Адже цілком правильним буде твердження, що сьогодні людини без інформації не існує. Тому забезпечення інформаційної безпеки кожної особи має стати невід'ємною частиною інформатизації світу загалом.

Актуальність обраної теми зумовлена постійними змінами в інформаційній сфері в умовах збройного конфлікту. У цій ситуації особливого значення в механізмі забезпечення інформаційної безпеки особи набуває діяльність держави та використання нею сучасних технологій.

На сьогоденність зазначеного питання вказує також і законопроєктна робота. Наразі в Україні висунуто декілька концепцій кодифікації інформаційного законодавства: проєкт Інформаційного кодексу України, проєкт модельного Інформаційного кодексу, проєкт Кодексу України про інформацію.

Аналіз останніх досліджень і публікацій. Правові питання забезпечення інформаційної безпеки особи в Україні досліджували різні вчені. Примітним є те, що це питання є предметом наукового пошуку в різних галузях права. Так, Т. Перун здійснив дослідження адміністративно-правового механізму забезпечення інформаційної безпеки в Україні, з'ясував і проаналізував концептуальні та організаційно-правові основи адміністративно-правового забезпечення інформаційної безпеки органами державної влади [1]. А. Нашинець-Наумова присвятила свою роботу питанням правового регулювання інформаційної безпеки [2]. Різними питаннями у сфері забезпечення інформаційної безпеки займається Б. Кормич, який присвятив дослідженню організаційно-правових основ політики інформаційної безпеки України свою докторську дисертацію [3]. В аспекті визначення науковців, які займалися означеною проблематикою, слід також згадати О. Довгань та Т. Ткачук та їхню роботу

«Система інформаційної безпеки України: онтологічні виміри» [4]. Окремо слід відзначити монографічну роботу О. Золотар «Інформаційна безпека людини: теорія і практика» [5]. Вказані праці мають велике наукове та практичне значення, однак зміни в суспільстві, настання епохи інформатизації потребують нового наукового пошуку.

Метою статті є аналіз правових аспектів забезпечення інформаційної безпеки особи в Україні.

Виклад основного матеріалу. Тріаду інформаційної безпеки можна показати в такий спосіб: інформаційна безпека держави, інформаційна безпека суспільства, інформаційна безпека особи. При цьому інформаційна безпека особи, суспільства та держави може забезпечуватися і на національному, регіональному, і на міжнародному рівнях. Нас цікавить питання забезпечення безпеки особи на державному рівні, зокрема правові аспекти такої діяльності в Україні.

Зауважимо, що інформаційна безпека особи має міждисциплінарне значення. Якщо говорити про науковий напрям, вона має кілька аспектів, зокрема правовий, адміністративний, економічний, психологічний, організаційно-технічний тощо. Однак за останній час в епоху розвитку інформаційного суспільства визначальне значення має правовий аспект забезпечення безпеки особи. Це питання і стане предметом нашого дослідження.

Стаття 17 Конституції України визначає, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [6]. Наведене законодавче положення свідчить, що інформаційна безпека за рівнем захисту належить до таких найважливіших цінностей, як державний суверенітет і територіальна цілісність. Цитоване положення підтверджує актуальність та затребуваність наукових пошуків у сфері забезпечення інформаційної безпеки держави.

Термін «інформаційна безпека» в Законі України «Про національну безпеку України» визначається як складова частина національної безпеки. У ст. 1 цього Закону національна безпека тлумачиться як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Об'єктами державної політики у сферах національної безпеки й охорони названо, зокрема, такі: «воєнна, зовнішньополітична, державна, економічна, інформаційна, екологічна безпека, кібербезпека України тощо». Наведене визначення фактично відносить інформаційне середовище до найважливіших державних пріоритетів у сфері національної безпеки і оборони [7].

Як уже було зазначено, питання закріплення терміна «інформаційна безпека» та засобів її забезпечення вирішується на рівні законопроєктної роботи. Так, у розділі XV «Інформаційна безпека як складова частина національної безпеки України» проекту Інформаційного кодексу вказано, що «інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації» [8].

Що стосується наукової сфери, наразі відсутня єдність точок зору щодо дефініції поняття «інформаційна безпека». Так, В. Ярочкін та Т. Шевцова в 1996 році визначили інформаційну безпеку як проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб'єктів, що беруть участь в інформаційній діяльності [9, с. 12]. Надане визначення, на наш погляд, не пройшло перевірку часом, і наразі воно більш тяжіє до визначення терміна «заходи забезпечення інформаційної безпеки».

На думку Р. Калюжного, інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [10, с. 20]. Автор розуміє інформаційну безпеку як вид суспільних правовідносин, тобто визначає предметом інформаційної безпеки відносини, що складаються між людьми.

Б. Кормич розуміє інформаційну безпеку як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, усього суспільства та держави [11, с. 268]. Фактично автор пропонує визначення інформаційної безпеки як певного стану правил здійснення інформаційних процесів.

А. Лукашов під час дослідження інформаційної безпеки в законодавстві Республіки Білорусь розтлумачує інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, що являють собою впорядковану сукупність інформаційних ресурсів, інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі [12]. Наведене визначення підтверджує, що інформаційна безпека має схоже визначення і в інших країнах.

О. Довгань та Т. Ткачук у своїй роботі відзначають, що «інформаційна безпека є системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема, політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо». Окремо автори зауважують, що в цьому аспекті важливим є розмежування «інформаційної безпеки» як стану динамічної системи та «забезпечення інформаційної безпеки» як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) [4, с. 100]. Ми цілком підтримуємо точку зору, що слід розрізняти поняття «інформаційна безпека» та «забезпечення інформаційної безпеки». Це різні дефініції, які визначають два різних правових явища: інформаційна безпека – це певний стан системи; забезпечення інформаційної безпеки – процес підтримання стану системи. Тобто забезпечення інформаційної безпеки завжди являє собою діяльність.

Наведені визначення надають можливість зробити проміжні висновки щодо тлумачення терміна «інформаційна безпека». Вказану дефініцію можна розуміти в декількох значеннях: як вид суспільних правовідносин, як захищеність встановлених законом правил здійснення інформаційних процесів, як стан динамічної інформаційної системи. Проведене дослідження надає можливість приєднатися до наукового визначення інформаційної безпеки як стану динамічної системи інформаційної безпеки. Таке тлумачення дозволяє одночасно надати дефініцію поняття інформаційної безпеки особи, суспільства та держави та не вимагає окремого виділення цих категорій.

Означивши як мету дослідження аналіз правових аспектів забезпечення інформаційної безпеки особи в Україні, слід перейти до аналізу чинників, які можуть становити загрозу інформаційній безпеці особи. У цьому аспекті слід враховувати, що ці фактори можуть бути і міждержавними, і внутрішньодержавними. Міждержавні пов'язані із наявними конфліктами у світі загалом, із наявністю збройного конфлікту на Сході України зокрема. Вважаємо, що це питання має наднаціональний характер і є предметом окремого дослідження.

Питання ж національних загроз інформаційній безпеці особи і правові шляхи їх вирішення пропонуємо розглянути більш детально.

По-перше, слід виділити таку загрозу інформаційній безпеці, як правовий вакуум у більшості питань забез-

печення інформаційної безпеки особи. У цьому аспекті під правовим вакуумом ми розуміємо відсутність єдиного нормативного акта, який би регламентував поняття інформаційної безпеки, її основні ознаки, засоби захисту, суб'єктів, на яких покладається обов'язок здійснювати захист тощо. Хоча законопроєктна робота в цьому напрямі ведеться, наразі не має можливості говорити про стадію прийняття Кодексу про інформацію. Способом протидії зазначеній загрозі, на наш погляд, є прийняття Кодексу України «Про інформацію».

По-друге, загрозою інформаційній безпеці особи є порушення законодавства з питань інформаційної безпеки. Хоча консолідований нормативний акт на сьогодні відсутній, існують правові норми, які фрагментарно регулюють питання забезпечення інформаційної безпеки.

До таких нормативних актів слід віднести:

– Кримінальний кодекс України (ст. 182 «Порушення недоторканності приватного життя», ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 362 «Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється» тощо [13];

– Кодекс України про адміністративні правопорушення (ст. 188-31 «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України», ст. 188-39 «Порушення законодавства у сфері захисту персональних даних» тощо [14]).

Способами протидії зазначеним загрозам, на наш погляд, має стати негайне звернення із заявою або повідомленням про кримінальне / адміністративне правопорушення до органів Національної поліції. Згідно з п. 5 ч. 1 ст. 23 Закону України «Про Національну поліцію» поліція здійснює реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події [15]. Окремо слід вказати на існування окремого спеціально уповноваженого органу – Кіберполіції України, завданням якого серед іншого є реалізація державної політики у сфері протидії кіберзлочинності [16]. Додамо, що у 2005 році Україна ратифікувала Конвенцію про кіберзлочинність і взяла на себе зобов'язання здійснювати погоджену політику боротьби зі злочинністю у цій сфері.

По-третє, загрозами інформаційній безпеці особи можуть бути відмови, зброї, технічні помилки інформаційних систем (засобів), а також природні процеси, що впливають на передачу, прийом і зберігання інформації. Способом протидії в цьому випадку може бути використання перевіреної техніки, заборона її використання сторонніми особами, очікування налагодження систем передачі інформації її володільцями.

По-четверте, загрозами можуть бути зовнішні чинники. В умовах збройного конфлікту все частіше трапляються випадки порушення інформаційної безпеки особи з боку Російської Федерації, зокрема розповсюдження антиукраїнських закликів, спам-повідомлення сепаратистського характеру тощо. Вчені зазначають, що подолати таку загрозу можна через захист українського суспільства від «агресивного інформаційного впливу Російської Федерації», розвиток публічної дипломатії, у тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту Інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо [4, с. 98].

Висновки. Забезпечення інформаційної безпеки особи в Україні має нерозривний зв'язок з інформаційним законодавством. Інформаційне законодавство та законодавство щодо інформаційної безпеки особи є відносно новою галуззю законодавства України й наразі перебуває тільки на етапі становлення. У цьому аспекті найбільш прийнятним варіантом його розвитку, на наш погляд, є розробка єдиного консолідованого нормативного акту, який визначить понятійний апарат; основні напрями державної політики щодо забезпечення інформаційної безпеки особи, суспільства та держави; об'єкти інформаційної безпеки; суб'єктів, на яких покладається обов'язок її забезпечення; основні загрози інформаційній безпеці та способи протидії тощо.

Правові питання забезпечення інформаційної безпеки особи безпосередньо пов'язані із визначенням загроз інформаційній безпеці особи і правових шляхів їх подолання. Першою загрозою є правовий вакуум у більшості питань забезпечення інформаційної безпеки особи, тобто відсутність єдиного нормативного акта, який би регламентував поняття інформаційної безпеки, її основні ознаки, засоби захисту, суб'єктів, на яких покладається обов'язок здійснювати захист тощо. Способом протидії зазначеній загрозі, на наш погляд, є прийняття Кодексу України «Про інформацію». Другою загрозою є порушення законодавства з питань інформаційної безпеки, зокрема порушення норм Кримінального кодексу України, Кодексу України про адміністративні правопорушення тощо. Способом протидії зазначеним загрозам має стати негайне звернення із заявою або повідомленням про кримінальне / адміністративне правопорушення до органів Національної поліції. Третьою загрозою є технічні помилки інформаційних систем (засобів), а також природні процеси, що впливають на передачу, прийом і зберігання інформації. Способом протидії в цьому випадку можуть бути використання перевіреної техніки, заборона її використання сторонніми особами, очікування налагодження систем передачі інформації її володільцями. Четвертою загрозою є зовнішні чинники. Подолати таку загрозу можна через захист українського суспільства від агресивного інформаційного впливу, розвиток публічної дипломатії тощо.

ЛІТЕРАТУРА

1. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. … канд. юрид. наук. Львів, 2019. 268 с.

2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.

3. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … док. юрид. наук : 12.00.07. Одеса, 2004. 427 с.

4. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. № 1(24). С. 89–103.

5. Золотар О.О. Інформаційна безпека людини:теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

6. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

7. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Офіційний вісник України*. 2018. № 55. Стор. 51. С. 1903.

8. Максименко Ю.Є. Щодо структури інформаційного кодексу України. URL : https://goal-int.org/shhodo-strukturi-informacijnogo-kodeksu-ukraini/ (дата звернення: 16.03.2020).
9. Ярочкин В.И. Словарь терминов и определений по безопасности и защите информации. Москва : Ось-89, 1996. 48 с
10. Калюжний Р. Питання концепції реформування інформаційного законодавства України. *Правове, нормативне та метрологічне забезпечення системи інформації в Україні: тематичний зб. праць учасників 2-ї науково-технічної конференції.* Київ, 2000. С. 17–21.
11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ : Кондор, 2004. 382 с.
12. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь: мат. научной конференции *«Концептуальные проблемы информационной безопасности в союзе России и Беларуси»*. Санкт-Петербург, 2000. URL : http://jurfak.spb.ru/conference/2001.htm (дата звернення: 16.03.2020).
13. Кримінальний кодекс України. *Відомості Верховної Ради України.* 2001. № 25. Ст. 131.
14. Кодекс України про адміністративні правопорушення. *Відомості Верховної Ради УРСР.* 1984. № 51. Ст. 1122.
15. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради.* 2015. № 40-41. Ст. 379.
16. Кіберполіція України. URL : https://cyberpolice.gov.ua/articles/ (дата звернення: 16.03.2020).