досліджень імені М.І. Долішнього НАН України»; за ред. С. Л. Шульц. Львів, 2018. 140 с. (Серія «Проблеми регіонального розвитку»).

3. Розказов А. Г. Особливості використання поняття «соціальний заклад»: публічно-управлінський аспект. Державне управління: удосконалення та розвиток. 2019. № 5. URL: www.dy.nayka.com.ua (дата звернення 01.09.2021)

4. Соціальні результати державних програм: теоретико-методологічні та прикладні аспекти оцінювання: [монографія] / за ред. Е.М. Лібанової; Інститут демографії та соціальних досліджень імені Птухи М.В. НАН України. Умань: Видавець «Сочінський», 2012. 312 с.

Швирло Юрій Михайлович
Головний державний інспектор сектору охорони державної таємниці, технічного та криптографічного захисту інформації
Головне управління ДПС у Тернопільській області

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасні тренди діджиталізації управлінських процесів та шляхів взаємодії суспільства і держави вимагають зосередження уваги на технологічних аспектах та програмнму забезпеченні методів захисту інформації. Сьогодні значну частину важливих даних (державна та комерційна таємниця, персональні дані тощо) вже оцифровано, однак обсяг такої інформації постійно зростає. Тому актуалізується питання її ефективного захисту, а також детального вивчення засобів і методів забезпечення такого захисту. У сучасний умовах надзвичайно важливо своєчасно оновлювати та модернізувати нормативно-правову та організаційну базу у цій сфері.

Різні аспекти організаційно-правових засад захисту інформації у своїх роботах розглядали І. Арістова, О. Олійник, Н. Новікова, І. Тацишин, Н. Нижник, В. Соловйов та ін. Водночас питання методів і засобів захисту інформації, а

також правові підстави їх використання у практичній діяльності потребують додаткового вивчення.

В Україні правові засади захисту інформації визначені у низці законів та нормативних актів, зокрема у Конституції України, Законі України «Про інформацію» від 02.10.1992 р., Законі України «Про державну таємницю» від 21.01.1994 р., Законі України «Про основи національної безпеки» від 19.06.2003 р., Стратегії національної безпеки України у сфері протидії інформаційним викликам тощо. Огляд цих документів дозволяє стверджувати, що основними напрямками діяльності щодо захисту інформації на національному рівні є захист інформаційного простору України та підвищення рівня освіченості держслужбовців щодо питань інформаційної безпеки [1]. Ці заходи повинні спрямовуватися переважно на реалізацію заходів щодо боротьби та протидії певним видам інформаційних війн, що передбачено Стратегією національної безпеки України [2]. Загалом сьогодні це завдання покладено на Міністерство інформаційної політики України.

Організаційне забезпечення цієї сфери передбачає створення ефективної системи захисту інформації, яка охоплює такі рівні:

1) адміністративний;

2) процедурний;

3) програмно-технічний.

Заходи адміністративного рівня передбачають формування політики інформаційної безпеки і визначення загальної структури системи захисту інформації. Тобто він включає правовий аспект й процедури, спрямовані на його реалізацію та досягнення інших цілей організації щодо безпеки даних. Формування політики інформаційної безпеки має базуватися, в першу чергу, на розумінні необхідності захисту інформації (яка саме інформація потребує захисту), а також на виокремленні рівнів захисту (наскільки цінною є інформація і, відповідно, якого рівня заходів слід вживати для її захисту). Зокрема, повинно бути чітко сформульовано розуміння того, яка інформація є публічною, а яка лише для внутрішнього використання.

Закон України «Про інформацію» від 02.10.1992 р. [4] визначає наступні види інформації із обмеженим доступом.

1. Конфіденційна – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

2. Таємна – інформація, доступ до якої обмежується виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя, розголошення якої може завдати шкоди особі, суспільству і державі.

3. Службова – інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи.

Процедурний рівень полягає у забезпеченні реалізації окремих процедур, спрямованих на реалізацію політики інформаційної безпеки. Цей рівень орієнтований переважно на регулювання щоденної діяльності окремих людей, залучених до роботи з інформацією. Тобто, на процедурному рівні визначається процес надання доступу; адміністрування доступів, наданих користувачам; проводиться навчання персоналу щодо правильного використання інформації, до якої надається доступ, а також щодо правильного використання програмного забезпечення.

Програмно-технічний рівень включає власне ресурсне забезпечення – наявність комп'ютерного та іншого технологічного обладнання (сервери, комп'ютери, мережеве обладнання), придбання (або розробку) і супровід програмного забезпечення (антивірусні програми, система контролю та управління доступом, шифрувальне програмне забезпечення, мережевий екран). Часто-густо саме цей рівень є основним при попередженні та виявленні

інформаційних загроз, оскільки більшість з них виникає у зв'язку із помилковими або несанкціонованими діями легальних користувачів інформації [3, с. 33-34].

Отже, у процесі дослідження організаційно-правових засад захисту інформації встановлено, що подальше забезпечення інформаційної безпеки на національному рівні вимагає вдосконалення правового регулювання, адекватної та своєчасної оцінки виду інформації та реалізації належних заходів її захисту відповідно до виду. З цією метою необхідно реалізувати належне методологічне та ресурсне забезпечення у цій сфері, що потребує спеціального розгляду та нових наукових розвідок.

Список використаних джерел

1. Пашковський В. Ф. Організаційно-правовий механізм забезпечення інформаційної безпеки України в умовах зовнішньої агресії: напрями вдосконалення. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право*. 2018. № 2. С. 29-33.

Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287/2015. URL: http://zakon2.rada.gov.ua/laws/show/287/2015 (дата звернення 05.05.2021).

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

3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 05.05.2021).