кандидат юридичних наук, старший науковий співробітник наукової лабораторії проблем протидії злочинам у сфері державної безпеки Інституту дослідження проблем державної безпеки СБ України

АДМІНІСТРАТИВНО-ПРАВОВА СУТНІСТЬ РЕЖИМУ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ, КРИПТОГРАФІЧНОГО І ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Стаття присвячена дослідженню адміністративно-правових аспектів режиму захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації. У роботі наведено авторське визначення такого режиму, правові межі його дії та основні аспекти адміністративної відповідальності за порушення вимог, правил та законодавства у сфері дії даного режиму, а також сформульовано пропозиції щодо її подальшого посилення.

Ключові слова: режим захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації; інформаційна безпека; інформаційні відносини; адміністративна відповідальність.

Статья посвящена исследованию административно-правовых аспектов режима защиты государственных информационных ресурсов, криптографической и технической защиты информации. В работе приведены авторское определение режима, правовые рамки его действия и основные аспекты административной ответственности за нарушение требований, правил и законодательства в сфере действия данного режима, а также сформулированы предложения по ее дальнейшему усилению.

Ключевые слова: режим защиты государственных информационных ресурсов, криптографической и технической защиты информации; информационная безопасность; информационные отношения; административная ответственность.

The article is devoted research of question in relation to the regime of defense of state informative resources cryptographic and technical priv from point of administrative law. Author determination of this regime, legal scopes of his action and basic aspects of legal administrative responsibility, is in-process resulted for violation of requirements, rules and legislation in the field of action of this regime, and also suggestions are given in relation to its further strengthening.

Key words: regime defense of state informative resources, cryptographic and technical priv; informative safety; informative relations; administrative responsibility.

Будь-яка сфера життя сучасного суспільства не може функціонувати без розвиненої інформаційної системи. Національний інформаційний ресурс є наразі одним із головних джерел економічної та військової потужності держави. Проникаючи в усі сфери діяльності держави, інформація набуває конкретних політичного, матеріального і вартісного виявів. На цьому фоні все більш актуального характеру набувають питання забезпечення інформаційної безпеки України як невід'ємного елементу національної безпеки, а захист інформації перетворюється на одне з пріоритетних державних завдань. У будь-якій державі інформаційній безпеці надається особливе значення. У своєму розвитку це завдання проходить безліч етапів залежно від потреб держави, можливостей, методів і засобів добування відомостей (зокрема, розвідки), правового режиму держави і реальних його зусиль щодо забезпечення захисту інформації.

Так, трансформаційний технологічний процес в інформаційній сфері зумовлює серйозні зміни в суспільстві в цілому. З часом змінюється спосіб життя

© Бєлєвцева В. В., 2011

мільйонів людей. Процеси глобалізації торкаються дедалі нових сфер діяльності, й інформаційна стає не тільки найважливішою сферою міжнародної співпраці, а й об'єктом безпекового сектору. Проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними загострюються внаслідок політичної й економічної нестабільності держави. Це стає актуальним, як зазначалося вище, в аспекті забезпечення безпеки держави.

Вагоме значення у дослідженні розглядуваного питання мають наукові праці В. М. Брижка, А. М. Гузя, О. П. Дзьобаня, В. В. Макаренка, А. І. Марущака, В. Я. Настюка, А. В. Пазюка, В. Г. Пилипчука, В. М. Поповича, В. С. Цимбалюка, М. Я. Швеця та ін. Проте в юридичній науці й досі має місце недостатність дослідження фундаментальних та прикладних проблем правового регулювання інформаційної сфери у цілому та окремих її складових, особливо з огляду забезпечення безпеки держави.

Метою даної статті є розгляд одного з головних завдань забезпечення національної безпеки в інформаційній сфері — захист державних інформаційних ресурсів, криптографічний і технічний захист інформації.

Визначальним і головним аспектом у процесі захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації є створення на шляху правопорушників надійних організаційно-правових бар'єрів, які б мінімізували, а й у ряді випадків повністю виключали можливість досягнення злочинних цілей відповідними суб'єктами. Тобто, іншими словами — встановлення відповідних адміністративно-правових режимів. У нашому випадку це й є правовий режим захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації.

У цілому слід відмітити, що державні інформаційні ресурси призначені для забезпечення національних інтересів України, захисту прав і свобод людини і громадянина, інтересів суспільства, органів державної влади та місцевого самоврядування, юридичних осіб в інформаційній сфері. Також вони виступають чинником захисту суверенітету й інформаційної безпеки держави, мають своє місце у площині вирішення завдань економіки, виробництва, науки, культури й інших сфер життєдіяльності суспільства. Узагалі, основним завданням нормального функціонування інформаційно-правового забезпечення державних інформаційних ресурсів є збереження відомостей, що є власністю держави, при дотриманні інформаційних прав і інтересів людини, громадянина та суспільства.

Інтереси людини і громадянина в інформаційній сфері полягають у реалізації конституційних прав людини і громадянина на доступ до інформації, використання інформації на користь здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку. Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особи в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні та підтримці суспільного миру. Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку української інформаційної інфраструктури, реалізації конституційних прав і свобод людини та громадянина у сфері отримання інформації і користування нею в цілях забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, політичної, економічної і соціальної стабільності, в безумовному забезпеченні законності й правопорядку, розвитку рівноправної і взаємовигідної міжнародної співпраці.

На основі перерахованих інтересів в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої

і зовнішньої політики держави щодо забезпечення інформаційної безпеки, визначаються види загроз інформаційній безпеці та їх джерела.

Аналізуючи наукові дослідження щодо розглядуваного питання доцільно відзначити, що базу державних інформаційних ресурсів, головним чином, формують:

– інформаційні ресурси Верховної Ради України, Адміністрації Президента України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду України, Національного банку України;

– інформаційні ресурси органів державної влади та органів місцевого самоврядування, державних установ, організацій, підприємств;

– інформаційні ресурси національної системи науково-технічної інформації;

– інформаційні ресурси Національного архівного фонду;

– інформаційні ресурси Музейного фонду;

– Національний електронний реєстр інформаційних ресурсів України;

– інші інформаційні ресурси або сукупності інформаційних продуктів, що мають державний статус відповідно до чинного законодавства України [1, с. 313–315].

Отже, відповідно до ст. 1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [2] державні інформаційні ресурси — це інформація, яка є власністю держави та необхідність захисту якої визначено законодавством.

Основні положення та види інформації, що є власністю держави і підлягає захисту, визначені у Конституції України, законах України «Про інформацію» та «Про державну таємницю».

Поняття криптографічного та технічного захисту інформації містяться у ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3], а саме:

– криптографічний захист інформації — це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– технічний захист інформації — це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

У цілому правовий режим захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації можна визначити як систему правових норм, організаційних та організаційно-технічних заходів, які регулюють діяльність, пов'язану з розробленням, дослідженням, виробництвом та експлуатацією засобів криптографічного та технічного захисту інформації з метою обмеження доступу до неї.

Правовою підставою даного режиму виступають Конституція України; закони України: «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Державну службу спеціального зв'язку та захисту інформації України»; положення: Про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису, Про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації тощо.

Органом, що регулює діяльність у сфері захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації, є Державна служба спеціального зв'язку та захисту інформації України. Це державний орган, призна-

чений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації. Діяльність Державної служби спеціального зв'язку та захисту інформації України спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування. Державна служба спеціального зв'язку та захисту інформації України підконтрольна Верховній Раді України.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є [2]:

– участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

– забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

– забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

– визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

– охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах регулює Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Інформаційна (автоматизована) система — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; інформаційно-телекомунікаційна система — сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [3].

Об'єктами захисту в цих системах є інформація, що обробляється в ній, та програмне забезпечення, призначене для обробки цієї інформації.

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

– власники інформації;

– власники системи;

– користувачі;

– спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації та мають своє відображення у ст. 4 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Отже, порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 9 вищезазначеного Закону регулює відносини щодо забезпечення захисту інформації в системі. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляється інформація, котра є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стосовно правопорушень щодо вимог та правил даного режиму можна навести таке. До них належать, на думку автора, такі протиправні діяння, які тягнуть за собою адміністративну відповідальність [4]:

– невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України (ст. 188^{31} Кодексу України про адміністративні правопорушення (КУпАП));

– незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації (ст. 195^{5} КУпАП);

– незаконний доступ до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212^{6} КУпАП).

З наведеного можна зробити висновок, що наявна адміністративна відповідальність не охоплює всі аспекти відносин у сфері дії режиму захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації, наприклад, порушення вимог та правил криптографічного і технічного захисту інформації; порушення вимог і правил збереження інформації в інформаційних (автоматизованих) системах або інформаційно-телекомунікаційних системах; порушення правил експлуатації (користування) державними інформаційними ресурсами та ін. Це призводить до послаблення охорони інформаційних відносин, прогалин та суперечностей у чинному законодавстві, а також малоефективного забезпечення інформаційної безпеки держави в цілому, оскільки довільне поводження у сфері режимно-інформаційних відносин може призвести до негативних або тяжких наслідків для безпеки держави.

На підставі викладеного вбачається за доцільне передбачити в законодавстві України окремо питання щодо:

– закріплення на законодавчому рівні поняття режиму захисту державних інформаційних ресурсів, криптографічного і технічного захисту інформації;

– удосконалення законодавства з метою посилення юридичної відповідальності за правопорушення у межах дії даного режиму.

Такий підхід дасть можливість запровадження більш ефективного адміністрування щодо дотримання порядку та законності у сфері інформаційних відносин. У загальнодержавному аспекті наведене зміцнить спроможність держави до за-

хисту всієї сукупності державних інформаційних ресурсів від зовнішніх та внутрішніх загроз та небезпек, а також її здатність зберігати та поновлювати інформаційний процес та достатній безпековий потенціал у кризових ситуаціях. Усі викладені проблемні питання, безумовно, потребують подальшого наукового дослідження з метою розробки конкретних практичних шляхів для їх вирішення.

Література

1. Правова інформатика : підручник : у 2 т. – К. : Парлам. вид-во, 2004. – Т. 1. – 416 с.
2. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // Відом. Верхов. Ради України. – 2006. – № 30. – С. 1094. – Ст. 258.
3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // Відом. Верхов. Ради України. – 1994. – № 31. – Ст. 286.
4 . Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X із змінами [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua.