licemen have to organize and practice in carrying out their daily work : workshops in labor collectives of enterprises, institutions and organizations of all patterns of ownership and educational institutions, hostels, stairs and duties of citizens, residents of residential areas, districts, settlements and villages; meetings with top (board) meeting of NGOs and their members (horticultural Society, the National Union of motorists, Union gardeners and vegetable growers, cooperatives, cottage owners and cottage gardens, etc.) meetings with the protection of private institutions and firms.

Key words: *public safety, public order, internal affairs bodies, warning, citizens.*

Стаття надійшла 09 квітня 2014 р.

УДК 342+35.083

В. Й. Шишко

СУТНІСТЬ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАХОДІВ ЗАХИСТУ СЛУЖБОВОЇ ІНФОРМАЦІЇ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

Досліджено актуальні питання сутності адміністративно-правових заходів захисту службової інформації в діяльності органів державної влади. На підставі теоретичного обґрунтування проаналізовано співвідношення понять «охорона» та «захист» інформації, визначено розуміння терміна «захист службової інформації» та його адміністративно-правову сутність, яка спрямована проти несанкціонованого доступу до цієї інформації. Визначено зміст адміністративно-правового захисту службової інформації, який ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини і спрямований проти несанкціонованого доступу до цієї інформації.

Ключові слова: *адміністративно-правові заходи, інформація, службова інформація, охорона, захист, криптографічний захист, документування.*

Постановка проблеми. Стан захисту державного інформаційного простору є одним із показників ефективності роботи держави щодо захисту власних інформаційних ресурсів від протиправних посягань. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути ефективні адміністративно-правові заходи.

Останнім часом в Україні відбуваються якісні зміни у процесах державного управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. У зв'язку із цим особливого значення набувають адміністративно-правові заходи захисту службової інформації.

Стан дослідження. Основу статті становить аналіз норм сучасного національного інформаційного законодавства, а також науковий доробок вітчизняних і зарубіжних учених, серед яких виокремимо А. О. Антонюка, В. М. Білоножко, К. В. Габучан, В. І. Даля, А. П. Загніткo, В. Н. Лопатина, А. І. Марущака, С. Ф. Ожегова, Л. М. Полюгу, В. Темченка, В. Ф. Шаньгина.

З уваги на зазначене, **метою** статті є визначення шляхів удосконалення адміністративно-правової охорони службової інформації та окреслення проблем, які перешкоджають належній реалізації адміністративно-правових заходів охорони службової інформації органів державної влади.

Виклад основних положень. Нормативно-правові акти надають різні визначення поняття «захист інформації», зокрема його визначають як сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією (п. 2.8 Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру, затвердженого наказом Ліцензійної палати при Мінекономіки України від 15.11.1996 р. № ЛП-37 [1]). Крім того, у Законі України «Про державну таємницю» від 21.01.1994 р. № 3855-XII [2] вживається термін «охорона державної таємниці» як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню таємної інформації та втратам її матеріальних носіїв. Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР [3] поняття «захист інформації в системі» розглядається як діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Крім того, законодавство не диференціює поняття «охорона» і «захист» інформації. Так, термін «охорона» у термінологічних слово-

сполученнях Конституції України вживається для позначення достатньо широкого кола повноважень державних органів, що передбачають, зокрема, запобігання правопорушенням, їх недопущення та відновлення прав і свобод у випадку їх порушення, а також притягнення винних до юридичної відповідальності. Особливістю застосування цього терміна у Конституції є його вживання зі значенням, аналогічним до терміна «захист», як обов'язку держави та інших зобов'язаних суб'єктів до дій щодо забезпечення прав і свобод людини [4, с. 63].

Отже, з огляду на зазначені визначення, можна констатувати, що терміни «захист» та «охорона» у нормативному контексті слід вживати як синоніми чи схожі за значенням поняття щодо мети, завдань, методів і суб'єктів забезпечення прав, тому вони можуть використовуватись у практиці як ідентичні поняття. Однак у науці інформаційного права вони не розглядаються як тотожні. Охорона інформації – встановлення її загального правового режиму, захист, заходи, які використовуються у тих випадках, коли суб'єктивні права на інформацію порушені або залишаються спірними. Проте в цій частині дослідження термін «захист інформації», на нашу думку, доцільно застосовувати в тому широкому значенні, яке йому надає законодавець. Воно охоплює і заходи, спрямовані на відвертання можливості неправомірних дій зі службовою інформацією, і заходи, спрямовані на захист і відновлення порушених прав.

Плутанина навколо понять «захист» та «охорона» прав цілком логічна з огляду на невизначеність цих понять і в тлумачних словниках. Зокрема, відповідно до Тлумачного словника В. Даля, «захист» – це заступництво [5, с. 542]. С. І. Ожегов визначає поняття «захищати» як «охороняючи, захистити від замахів, від ворожих дій, від небезпеки» [6, с. 196]. Водночас слово «охорона» означає «берегти, оберігати, захищати, тримати в цілісності, рятувати» [7, с. 774], а також «стежити, щоб не зробили шкоди кому-небудь або чому-небудь» [8, с. 234]. Отож, захист у соціально-філософському розумінні становить охорону, а охорона, своєю чергою, – захист. Зауважимо, що в словнику синонімів [9, с. 322] досліджувані поняття також вживаються як синоніми, тобто можуть бути взаємнозамінюваними залежно від контексту. Проте в деяких тлумачних словниках указується, що захист чого-небудь здійснюється в процесі охорони, в той час як «охороняти» визначається як «ставитися з обережністю, берегти». Цікаво і те, що в словнику української мови «захист» визначається як заступництво, охорона, підтримка [10, с. 99].

У тлумачному словнику сучасної інформаційно-правової лексики захист інформації розглядається з п'яти позицій:

1) як діяльність, спрямована на забезпечення конфіденційності, цілісності й доступності інформації;

2) як сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації в умовах впливу на неї загроз природного й штучного характеру, реалізація яких може призвести до заподіяння шкоди власникам чи користувачам інформації;

3) як комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На практиці під цим розуміється підтримка цілісності, доступності і, якщо потрібно, конфіденційності інформації і ресурсів, що використовуються для введення, збереження, обробки і передачі даних;

4) як діяльність, спрямована на збереження державної, службової (комерційної) або особистої таємниці, а також на збереження носія інформації будь-якого змісту;

5) як використання в системах збору, передачі, збереження і переробки інформації спеціальних методів і засобів з метою забезпечення схоронності інформації, що захищається, і запобігання витоку технічними каналами [11, с. 147].

Отже, нормативно-правове розуміння адміністративно-правових заходів захисту інформації, зокрема службової, зводиться до системи правових, організаційних, інженерних, технічних заходів, що спрямовані на збереження цілісності службової інформації та запобігання її витоку.

Тому зміст адміністративно-правового захисту службової інформації ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини.

А. О. Антонюк відносить до сфери безпеки інформації не захист інформації, а захист права власності на неї [12, с. 103]. Справді, захист інформації організовує і здійснює власник, користувач інформації або уповноважена ними особа (фізична чи юридична), а також держава в особі компетентних органів у межах своєї правоохоронної функції. Захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, намагається запобігти незаконному заволодінню нею і використанню її на шкоду власним інтересам. Система захисту може бути різна, на розсуд власника, а може і не мати такого захисту взагалі. Він здійснюється на основі диспозитивних методів, що входять у сферу цивільно-правового розгляду. Захист інформації стає

предметом адміністративно-правового регулювання у випадках, коли обмеження доступу до інформації прямо передбачені законами, коли ці обмеження пов'язані із забезпеченням інформаційних прав і свобод людини, інформаційних аспектів національної, державної, громадської безпеки, моральності, громадського здоров'я тощо і, що дуже важливо, суб'єктом застосування цих обмежень є держава в особі її компетентних органів [13, с. 108].

Від поняття «захист інформації» слід відмежувати захист інформаційних прав особи. У визначенні, що надається А. І. Марущаком, «суб'єктивне право на інформацію – гарантована державою можливість фізичних осіб і держави (державних органів) вільно одержувати, використовувати, поширювати та зберігати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права і інтереси юридичних осіб». Отож, у поняття «захист інформаційних прав особи» входить комплекс можливих видів інформаційної діяльності, де захист інформації є лише однією зі складових. З погляду теорії права, об'єктами правового захисту є права і законні інтереси, зокрема право на інформацію [14, с. 42]. Як стверджує В. Н. Лопатін, «сама інформація не може мати прав та інтересів, а її захист (організаційними, технічними іншими засобами) може і повинен залишатися умовами охорони права на інформацію (наприклад, стосовно інформації з обмеженим доступом)» [15, с. 91].

З уваги на наведене, на нашу думку, поняття «охорона» і «захист» інформації можна визначити як комплекс дій власника інформації для забезпечення прав на її володіння і розпорядження, а також сприяння життєдіяльності людини, суспільства і держави на основі створення органами управління безпечних умов, що обмежують розповсюдження і виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Форми адміністративно-правового захисту службової інформації традиційно можна класифікувати на юрисдикційні і неюрисдикційні. До одних належить захист порушених прав суб'єктів інформаційних правовідносин у судовому та адміністративному порядку. До інших – організаційні, технічні, криптографічні адміністративно-правові засоби захисту службової інформації.

Механізм захисту службової інформації є певним поєднанням організаційних, технічних, криптографічних і юрисдикційних засобів захисту інформації. Усі вони є правовими, оскільки встановлюються

правовими актами управління, зокрема нормативно-правовими. Адміністративно-правовий захист службової інформації – це діяльність щодо застосування юрисдикційних і неюрисдикційних форм її захисту.

Різноманітні моделі і рекомендації щодо створення системи організаційних заходів захисту службової інформації ґрунтуються на універсальному комплексі послідовних заходів:

– формування служби інформаційної безпеки або призначення особи (групи осіб), відповідальної за забезпечення інформаційної безпеки в цій структурі органу виконавчої влади;

– призначення відповідальних осіб у виділених приміщеннях, на конкретних інформаційних об'єктах, а також у приміщеннях, де зберігається службова інформація, зокрема на паперових носіях;

– розробка і затвердження плану заходів щодо забезпечення інформаційної безпеки (річного, квартального, місячного тощо);

– конкретизація плану з певною метою, завданнями, місцем і часом здійснення заходів;

– навчання, підвищення кваліфікації фахівців щодо забезпечення захисту службової інформації, контроль за рівнем їх підготовки з огляду на можливості бюджетного фінансування.

Вказані плани і заходи щодо організаційного забезпечення безпеки інформації, безумовно, мають свою специфіку щодо окремих видів інформаційних ресурсів і регламентуються підзаконними нормативно-правовими актами, які, як правило, мають гриф обмеження доступу.

Проте на рівні законів визначаються загальні напрями комплексу адміністративно-правових заходів щодо забезпечення захисту службової інформації, які повинні створювати основу для використання технічного, криптографічного та інших адміністративно-правових заходів захисту службової інформації, спрямованих проти несанкціонованого доступу до цієї інформації, проти її спотворення, блокування, знищення.

Так, діяльність щодо технічного захисту службової інформації, що підлягає ліцензуванню, повинна відповідати таким вимогам: наявність спеціальної освіти у осіб, що її здійснюють, або наявність у них спеціальної підготовки; відповідність виробничих приміщень, виробничого, випробувального і контрольно-вимірювального устаткування технічними нормами і вимогами, встановленими державними стандартами і нормативно-методичними документами щодо технічного захисту службової інформації; використання сертифікованих (атестованих

за вимогами безпеки інформації) автоматизованих інформаційних систем і засобів їх захисту; використання третіми особами програм для ЕОМ або баз даних на підставі договору з їх правовласниками.

Ще один адміністративно-правовий захід захисту службової інформації – криптографічний, який є захистом інформації за допомогою шифрувальних засобів (криптографічні засоби захисту інформації – КСЗІ) [16, с. 32], повинен здійснюватися на підставі спеціальної Інструкції, що визначає порядок організації і забезпечення безпеки зберігання, обробки, передачі каналами зв'язку з використанням криптографічних засобів захисту інформації обмеженого доступу, державною таємницею. Зазначимо, що ліцензіати відповідно до цієї інструкції зобов'язані забезпечувати комплексність захисту конфіденційної інформації, тобто використовувати інші засоби захисту, окрім криптографічних, в їх оптимальному поєднанні. Так, наприклад, усі співробітники органів криптографічного захисту інформації зобов'язані дотримуватись вимог щодо надійного зберігання експлуатаційної і технічної документації, ключових документів (ключів, шифрів), негайно вживати заходів щодо відвертання та просочування інформації у разі втрати, розкрадання, недостачі КСЗІ, ключів, шифрів посвідчень, пропусків тощо. Порушені права можуть бути відновлені також у результаті розгляду судом заяви громадянина про неправомірність дії посадовця або колегіального органу. До юрисдикційних форм захисту належать застосування кримінальних, адміністративних, а також дисциплінарних санкцій.

Що стосується юрисдикційних форм реалізації адміністративно-правових заходів захисту службової інформації у сфері діяльності публічної влади, то, на нашу думку, вони повинні реалізовуватися з метою відновлення порушених прав суб'єктів інформаційних правовідносин. До таких заходів насамперед слід віднести:

– документування службової інформації, що є основою для реєстрації інформаційних ресурсів;

– обмеження доступу до службової інформації, що забезпечується системою їх захисту;

– правовий захистслужбової інформації, що виражається існуванням інституту адміністративно-правової відповідальності за порушення законодавства про службову інформацію, який є однією з гарантій належної її реалізації та правового захисту.

Найменш урегульованим є порядок реєстрації баз, банків даних у частині визначення права власності на ці ресурси і порядок обліку їх

у складі державного майна. З метою удосконалення цієї проблеми необхідна систематизація адміністративного законодавства в частині об'єднання норм, які встановлюють адміністративно-правову відповідальність за правопорушення, предметом посягання яких може бути службова інформація.

Висновок. З метою обґрунтування власної позиції зазначимо, що адміністративно-правові заходи захисту службової інформації можна визначити як сукупність методів, засобів і прийомів, спрямованих на забезпечення інформаційної безпеки людини, суспільства і держави у всіх сферах їх життєво важливих інтересів. Сутність їх полягає у виявленні, вилученні і нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації, а цілі і заходи адміністративно-правового захисту службової інформації повинні здійснюватися з огляду на її зміст.

1. Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру: наказ Ліцензійної палати при Мінекономіки України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0693-96

2. Про державну таємницю: Закон України від 21.01.1994 р. № 3855. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12

3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

4. Темченко В. Особливості юридичного змісту термінів «захист» та «охорона» у механізмі забезпечення прав людини / В. Темченко // Вісник Академії управління МВС. – 2007. – № 2–3. – С. 58–65.

5. Даль В. Толковый словарь живого великорусскогоязыка: в 4 т. / В. Даль. – М.: Русский язык, 1999. – Т. 1: А–З. – 1999. – 699 с.

6. Ожегов С. И. Словарь русского языка / С. И. Ожегов; под ред. д-ра филол. наук, проф. Н. Ю. Шведовой. – М.: Русский язык, 1984. – 797 с.

7. Даль В. И. Толковый словарь живого великорусского языка / В. И. Даль. – Т. 2. – М.: Русский язык, 1979. – 780 с.

8. Габучан К. В. Учебный толковый словарь русского языка / К. В. Габучан. – М.: Русский язык, 1988. – 441 с.

9. Полюга Л. М. Словник синонімів української мови / Левко Михайлович Полюга; НАН України; Інститут українознавства ім. І. Крип'якевича; Український мовно-інформаційний фонд. – 3-тє вид. – К.: Довіра, 2007. – 477 с.

10. Білоножко В. М. Великий тлумачний словник сучасної української мови / В. М. Білоножко, А. А. Бурячок, Г. М. Гнатюк та ін.; Інститут української мови НАН України; Інститут мовознавства НАН України; Всеукраїнське товариство «Просвіта» ім. Тараса Шевченка. – К.: Дніпро, 2009. – 1332 с.

11. Загнітко А. П. Тлумачний словник сучасної української мови / А. П. Загнітко, І. А. Щукіна. – Донецьк: БАО, 2009. – 960 с.

12. Антонюк А. О. Основи захисту інформації в автоматизованих системах: навч. посіб. / А. О. Антонюк. – К.: КМ Академія, 2003. – 244 с.

13. Марущак А. І. Інформаційне право: доступ до інформації: навч. посібник / А. І. Марущак. – К.: КНТ, 2007. – 532 с.

14. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: навч. посібник / А. І. Марущак. – К.: Скіф; КНТ, 2008. – 343 с.

15. Лопатин В. Н. Правовая охрана и защита служебной тайны / В. Н. Лопатин // Государство и право. – 2000. – № 6. – С. 88–93.

16. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: уч. пособ. / В. Ф. Шаньгин. – М.: Форум, 2008. – 416 с.

Шышко В. И. Сущность административно-правовых мер защиты служебной информации в деятельности органов государственной власти

Исследованы актуальные вопросы сущности административно-правовых мер защиты служебной информации в деятельности органов государственной власти. На основании теоретического обоснования проанализировано соотношение понятий «охрана» и «защита» информации, определено понимание термина «защита служебной информации» и его административно-правовая сущность, которая направлена против несанкционированного доступа к этой информации. Определено содержание административно-правовой защиты служебной информации, которое отождествляется с процессом обеспечения информационной безопасности как необходимости нормального функционирования государства, общества, отдельного человека и направлено против несанкционированного доступа к этой информации.

Ключевые слова: *административно-правовые меры, информация, служебная информация, охрана, защита, криптографическая защита, документирование.*

Shyshko V. I. The essence of the legal and administrative measures to protect insider information in the public authorities activities

The article deals with the current issues of the administrative and legal measures nature to protect insider information in the work of the public authorities, which is one of the indicators of the effectiveness of the state to protect their information resources against unlawful encroachments.

It is analyzed in the context of the regulatory relationship between the concepts «protection» and «defense» of information based on the theoretical study, which in my opinion should be taken as synonyms or similar in the meaning about the purpose, objectives, methods and subjects of the rights of individuals and legal entities.

Administrative and legal protection content of the insider information, which is identified with the process of the information security as necessary, the proper

functioning of the state, society, and the individual is directed against unauthorized access to this information.

The author determined forms of the administrative and legal protection of the insider information, which can be classified into traditional jurisdictional and non jurisdictional.

We prove that the legal and administrative measures to protect insider information is a set of the methods, tools and techniques to ensure information security for man, society and the state in all areas of their vital interests. The essence of them is to identify, extract and neutralize the negative sources, causes and conditions of the exposure to information.

Key words: *administrative and legal measures, information, insider information, protection, cryptographic protection, documentation.*

Стаття надійшла 26 березня 2014 р.