*УДК 342.9:004(477)*

***Віталій Терехов,***
*здобувач Міжрегіональної Академії управління персоналом*

# УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ РЕАЛІЗАЦІЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ

*Досліджено особливості нормативно-правового регулювання забезпечення інформаційної безпеки в органах місцевого самоврядування. Виокремлено фактори, що впливають на стан захищеності інформації в органах місцевого самоврядування, а також потенційні ризики, які можуть завдати шкоду муніципальному інформаційному середовищу. У висновку констатовано відсутність системного правового уявлення про інформаційну безпеку та суб'єктів її забезпечення на місцях у вітчизняному адміністративно-правовому регулюванні. Запропоновано розробити концепцію інформаційної безпеки органів місцевого самоврядування.*

***Ключові слова:*** *інформаційна безпека, захист інформації, органи місцевого самоврядування, інформаційні загрози, регіональні програми інформатизації.*

***Терехов В.***

***Усовершенствовали административно-правового регулирования реолизации политики информационной безопасности в органах местного самоуправления***

*Исследовано особенности нормативно-правового регулирования обеспечения информационной безопасности в органах местного самоуправления. Выделено факторы, влияющие на состояние защищенности информации в органах местного самоуправления, а также потенциальные риски, которые могут нанести вред муниципальной информационной среде. В заключении констатируется отсутствие системного правового представление об информационной безопасности и субъектов ее обеспечения на местах в отечественном административно-правовом регулировании. Предложено разработать концепцию информационной безопасности органов местного самоуправления.*

***Ключевые слова:*** *информационная безопасность, защита информации, органы местного самоуправления, информационные угрозы, региональные программы информатизации.*

***Terehov V.Y.***

***Legal improvement of information security policyin local governments***

*In the article, the author researched the peculiarities of the regulatory and legal regulation of the provision of information security in local self-government bodies. The author highlighted the factors which affect to the local information security. Also, author separated potential risks that could damage the municipal information environment. In conclusion, the author noted the lack of legal consistencyof information security and their subjects in the domestic legal regulation. As a result, the author proposed to develop the concept of information security of local authorities.*

***Keywords:*** *information security, information protection, local self-government bodies, information threats, regional informatization programs.*

В сучасних умовах активного розвитку інформатизаційних процесів, переходу на електронне урядування, електронну демократію та документообіг, а також у зв'язку із впровадженням нових інформаційних систем в діяльність місцевого самоврядування питання забезпечення інформаційної безпеки та захисту інформації набуває все більшої актуальності не тільки в технологічному аспекті, а й в середовищі державно-правового регулювання. На сьогодні є чітке розуміння того, що процедури забезпечення інформаційної безпеки рефлектні багатьом факторам, які часто не пов'язані із технічними особливостями процесів інформаційно-телекомунікаційного середовища, що вимагає комплексності їх вивчення.

У правовій доктрині дослідження інформаційної безпеки не є чимось новим з позиції новизни. Багато вітчизняних вчених приділили значну увагу до висвітлення теорії безпечності інформаційних відносин. Необхідно відзначити таких вчених, як: Я. Малик, Ф. Ведмідь, О. Голобуцький, А. Новицький, П. Друкер, С. Галушко, І. Арістова, В. Бебик, А. Гальчинський, О. Олійник та ін. Проте в більшості випадків у цих дослідженнях відзначається направленість предмету на відносини, що виникають з приводу забезпечення інформаційної безпеки в органах державної влади загалом. При цьому зовсім мало праць присвячено аналізу зазначеного виду безпеки саме в контексті функціонування конкретного відомства чи органу. Вивчення інформаційної безпекової діяльності та політики правового забезпечення захисту інформації в органах місцевого самоврядування дасть можливість не тільки доповнити концепт національної інформаційної безпеки, а й окреслити практичні напрямки його локальної реалізації.

Незважаючи на активну децентралізацію влади, інформаційна безпека органів місцевого самоврядування (на відміну від інших видів безпек) не є самостійно-відірваним об'єктом від усього національного інформаційного простору. Вона не залежить від факторів та чинників, які зумовлені кліматичними показниками чи демографічним станом. Як правило, інформаційні небезпеки на місцях – це відлуння загальних проблем інформатизації, що існують в державі, а тому для їх вирішення у першу чергу необхідно удосконалювати підходи до загальнодержавного інформаційного захисту.

Основу нормативно-правового регулювання питання інформаційної безпеки становлять загальнодержавні нормативні акти, а відтак правове забезпечення місцевої політики інформаційної безпеки та протидії загрозам інформаційного середовища має чітко узгоджуватися з ними. Таким чином, підтримується єдність національного інформаційного простору.

На теренах ЄС є чимало нормативних актів, які встановлюють стандарти інформаційної безпеки в органах місцевого самоврядування. Новий підхід у розумінні сутності інформаційної безпеки та захисту інформації у мережі в умовах глобалізації було запропоновано у Резолюції Ради Європи 2002/С 43/02. Ідея документа спрямована на вироблення загальних підходів та конкретних дій у сфері мережевої та інформаційної безпеки. До речі, складові елементи категорії «інформаційна безпека» (забезпечення доступності послуг та даних; запобігання порушенням та несанкціонованим перехопленням комунікаційних технологій; верифікація повноти та незмінності відправлених, отриманих або збережених даних; забезпечення конфіденційності даних, захист інформаційних систем від несанкціонованого доступу; захист інформаційних систем від атак із застосуванням шкідливого програмного забезпечення; забезпечення надійної автентифікації суб'єктів інформаційної взаємодії [8]), що запропоновані в Резолюції, можна використовувати і у вітчизняному інформаційному законодавстві.

Основи інформаційної безпекової діяльності в Україні закладено в Конституції України. Так, у ст. 17 Основного Закону зазначається, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1]. Забезпечення інформаційної безпеки України – це, відповідно до ч. 1 ст. 3 Закону України «Про інформацію», основний напрямок державної інформаційної політики [4]. Згідно зі ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», комплексна система захисту інформації, у тому числі, в органах місцевого самоврядування, є взаємопов'язаною сукупністю організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, що являє собою діяльність, спрямовану на протидію несанкціонованим діям щодо інформації в системі [3].

Інший документ, на який необхідно звернути увагу з огляду на дослідження питання забезпечення інформаційної безпеки на місцях, є Стратегія кібербезпеки України, що затверджена Указом Президента України № 96/2016 від 15.03.2016 [7]. Беззаперечно, кіберпростір є сучасною площиною забезпечення реалізації інформаційних процесів у електронній формі, а тому його захищеність, зокрема у контексті діяльності органів місцевого самоврядування, є елементом стратегії місцевої інформаційної безпеки. У зазначеній вище Стратегії органи місцевого самоврядування визначені як обов'язковий елемент системи кібербезпеки, що покликані взаємодіяти з державними органами, військовими формуваннями, правоохоронними органами, науковими установами, навчальними закладами, громадськими об'єднаннями, а також підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [7]. На наш погляд, у згаданій Стратегії доцільним було б розкриття механізму взаємодії органів місцевого самоврядування з іншими суб'єктами забезпечення кібербезпеки, що суттєво підвищить ефективність акту загалом та створить підгрунтя для розробки нормативного забезпечення місцевого значення.

Одним із найважливіших атрибутів інформаційних правовідносин є їх захищеність. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» закріплено правовий статус таких видів захисту як криптографічний та технічний [3]. Але зазначені переліки не охоплюють весь обсяг методів, способів захисту інформації від загроз та небезпек, що циркулюють та можуть виникати на обмеженій території. Незважаючи на те, що формальної згадки про участь органів місцевого самоврядування у питаннях організації захисту інформаційних потоків у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» немає, відповідно до ст. 30 Закону України «Про місцеве самоврядування» до відання виконавчих органів сільських, селищних, міських рад віднесено сприяння діяльності Державної служби спеціального зв'язку та захисту інформації України [5]. На наш погляд, таке положення потребує більш детального роз'яснення, зокрема, щодо механізму взаємодії. Тому є необхідність розробки

спільних меморандумів взаємодії органів місцевого самоврядування та підрозділів Державної служби спеціального зв'язку та захисту інформації України у питаннях захисту інформації.

Більш детально необхідно зупинитися на загальній стратегії інформаційної безпеки, система якої формально проголошена в Національній програмі інформатизації. Згідно зі ст. 5 Закону України «Про Національну програму інформатизації», головною метою процесів інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [6]. Зазначений вище Закон є досить важливим елементом системи інформаційної безпеки навіть незважаючи на те, що приписної конструкції про роль та участь органів місцевого самоврядування у ньому немає. Справа в тому, що ст. 17–19 Закону створюють правові підстави та закріплюють за суб'єктами інформаційних відносин у державі (центральними органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями) обов'язок розробки та прийняття програм інформатизації, що за великим рахунком, є сукупністю стратегій та правових інструментів для формування політики інформаційної діяльності відповідно до власних потреб кожного суб'єкта. Питання інформаційної безпеки не є виключенням.

Згідно зі ст. 2 означеного Закону, Національна програма інформатизації, серед іншого, включає в себе програми та проекти інформатизації органів місцевого самоврядування, які ними ж розробляються і після погодження з Генеральним державним замовником Національної програми інформатизації [6] підлягають виконанню.

Беручи до уваги положення ст. 6 Закону України «Про Національну програму інформатизації», у якій стверджується, що функцією саме органів державної влади є забезпечення інформаційної безпеки, вважаємо, що зазначене формулювання назви статті не охоплює загалом органів місцевого самоврядування як невід'ємних суб'єктів забезпечення інформаційної безпеки. А тому пропонується відкорегувати назву ст. 6 Закону України «Про Національну програму інформатизації» та запропонувати її наступну редакцію: «Стаття 6. Функції державних органів та органів місцевого самоврядування у реалізації Національної програми інформатизації».

Важливо також звернути уваги на підзаконне нормативно-правове регулювання у сфері інформатизаційних процесів на місцях. Так, типові проекти інформатизації в областях, районах, (містах) розробляються та приймаються на основі Постанови Кабінету Міністрів України № 644 від 12 квітня 2000 р. «Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації». На підставі аналізу деяких місцевих Програм інформатизації приходимо до висновку про наявність у них недоліків, що мають бути усунені шляхом внесення змін до Порядку формування та виконання регіональної програми і проекту інформатизації.

По-перше, констатується відсутність системного правового уявлення про інформаційну безпеку та суб'єктів її забезпечення, а також не прослідковується зв'язок положень програми із приписами загальних стратегічних актів-документів загальнодержавного характеру в розрізі аналізу питань програми інформатизації. У зв'язку з цим, пропонується в обов'язковому порядку розробляти питання інформаційної безпеки, яке необхідно формалізувати в конкретних завданнях з інформатизації. Для цього в Додатку 1 до Порядку формування та виконання регіональної програми і проекту інформатизації у примітках (Завдання повинні охоплювати такі питання) необхідно доповнити наступне питання: «Заходи забезпечення інформаційної безпеки».

По-друге, слід зауважити про необхідність перегляду строків стратегії реалізації програм інформатизації, які згідно з п. 3 досліджуваного Порядку становлять 3 роки. З урахуванням швидкої динаміки розвитку інформаційно-телекомунікаційних процесів та стандартів інформаційної безпеки, строк 3 роки рекомендується скоротити до 2-х. У ході аналізу деяких програм інформатизації на місцях (наприклад, програми інформатизації Дніпровської міської ради на 2016–2020 р. [2]) було також встановлено недотримання строків при розробці та прийняті програм. А тому необхідно забезпечити організацію контролю за реалізацією приписів Програми формування та виконання регіональної програми і проекту інформатизації спеціально створеною комісією при органах місцевої влади, яка включала б фахівців у сфері інформаційного захисту, громадськість, уповноважених осіб органів влади, представників місцевих правоохоронних органів тощо.

Незважаючи на те, що з позиції інформаційно-телекомунікаційного простору муніципальна безпека є складовим елементом національної загальнодержавної інформаційної безпеки, тим не менш, вона має свої специфічні ознаки, які суттєвим чином можуть впливати на стан інформаційної захищеності в

органах місцевого самоврядування. До загальних чинників, що можуть у тій чи іншій мірі впливати на стан місцевої інформаційної безпеки, слід віднести: 1) наближеність до кордону (у цьому випадку особливо яскравим прикладом слугує стан неоголошеної інформаційної війни на прилеглих до зони бойових дій територіях Донецької та Луганської областей, де транслюються недостовірні відомості та інформація про події в Україні та прилеглих територіях, що направлені на дискредитацію влади); 2) рівень розвитку інформаційно-телекомунікаційних систем органів місцевого самоврядування, їх інтегрованість в загальнонаціональний інформаційний простір; 3) переважання обсягу паперового документообігу над електронним; 4) забезпеченість персональними робочими станціями, законність використання програмного забезпечення (його ліцензованість та сертифікованість), наявність корпоративної захищеної мережі обміну, збереження та накопичення інформаційних ресурсів); 5) наявність спеціалізованого програмного забезпечення для адміністрування власних баз даних; 6) напружена політична ситуація, яка може провокуватись виборчим процесом або самими діями представників місцевих органів влади; 7) використання (або невикористання) в постійному режимі місцевої PR інформаційної політики; 8) загальні показники інформатизованості місцевого населення, їх активність у муніципальному житті; 9) наявність прозорих та автономних місцевих засобів масової інформації, їх пов'язаність із представниками місцевої влади; 10) наявність фактів втручань та переслідування громадських активістів, журналістів, місцевого населення за їх інформаційно-поширюючу діяльність, відсутність притягнень до відповідальності за протиправну діяльність; 11) низький рівень правового регулювання основ інформаційних відносин та процесів в приватному секторі, що комунікує із представниками місцевої влади, правоохоронними органами та іншими суб'єктами забезпечення безпеки.

До вищезазначеного слід додати, що для кожного муніципального учасника характерні свої загрози та ризики у сфері нормального функціонування інформаційної інфраструктури, які існують як в середині, так і ззовні інформаційного поля. Проте всі інформаційні небезпеки, що можуть виникати в ході інформаційної діяльності суб'єктів муніципальних відносин, мають певну схожість. На наш погляд, з метою групування за природою ризиків необхідно вдатися до виокремлення інформаційної ролі (статусу) таких суб'єктів, тобто «виробників» (тих, які створюють відомості та інформацію в якості продукту) та «користувачів» як споживачів такої інформації. Особливою інформаційною роллю наділені органи місцевого самоврядування як «координатори» інформаційної взаємодії, тобто пов'язуюча ланка комунікації між усіма учасниками інформаційної системи. Саме для них буде характерна потрійна інформаційна роль як виробника, користувача, так і посередника. Звичайно, що така класифікація є умовною і за певних обставин роль одного суб'єкта може трансформуватись до іншого і навпаки. Наприклад, «виробник» інформаційного продукту – місцеве населення, а правоохоронний орган, якому надійшла конфіденційна інформація – споживач, який зобов'язаний вжити заходів зі збереження, нерозголошення такої інформації та використання її виключно на благо особи та суспільства. З іншого боку, правоохоронний орган може виступати виробником відомостей, наприклад, про результати здійснення контролю за дотриманням місцевого громадського порядку та безпеки. У цьому випадку його завдання полягає у наданні достовірної, правдивої, неупередженої та повної інформації. З-поміж іншого, для органів місцевого самоврядування можуть бути характерні такі інформаційні загрози: несанкціоноване поширення відомостей, які перебувають в обігу органів місцевої влади; відсутність єдиного захищеного каналу зв'язку із комунальними підприємствами, правоохоронними органами тощо; факти дискредитації роботи місцевих органів в мережі Інтернет на соціальних порталах та форумах; незабезпеченість (низький рівень забезпеченості) персональними робочими станціями, безперебійним та надійним доступом до мережі Інтернет; поширення недостовірних відомостей про діяльність посадових осіб місцевих органів та інформаційний тиск.

І насамкінець, окрім інформаційних загроз, які повинні бути враховані суб'єктами інформаційних відносин на місцях при розробці програм інформатизації, необхідно з'ясувати об'єкти інформаційного захисту. Загалом всі елементи, через які проходять потоки інформації, будь-які елементи, де інформація накопичується та поширюється далі, можна однозначно віднести до об'єктів, що потребують захисту або хоча б уваги. З теоретико-методологічного підходу розроблено не один критерій щодо класифікації потенційних інформаційних об'єктів захисту. Але фокусуючись на обмеженій території та з урахуванням сучасного вітчизняного стану розвитку інформаційних, технологічних систем і нерівномірних особливостей розвитку регіонів, пропонується при розробці концепції інформаційної безпеки на місцях акцентувати увагу на наступних об'єктах системи загалом: програмне забезпечення; соціальні медіа; системи накопичення та збереження даних; системи обробки, кодування та поширення інформації; бази даних; апаратна інфраструктура; корпоративні внутрішні мережі; місце збереження та обігу паперової інформації тощо.

Отже, інформаційна безпека в органах місцевого самоврядування – це складний механізм забезпечення технологічного функціонування інформаційної системи в органах місцевого самоврядування, а також протидія її небезпекам, загрозам та ризикам.

З урахуванням високої динаміки інформатизаційних процесів, що здатні суттєво порушувати інформаційно-телекомунікаційне муніципальне середовище та несистемності положень підзаконних нормативних актів, рекомендується розробити концепцію інформаційної безпеки в органах місцевого самоврядування.

**Список використаної літератури**

1. *Конституція України : Закон України № 254к/96-ВР від 28.06.1996 р. // Відомості Верховної Ради України (ВВР) – 1996 – № 30 – ст. 141. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.*
2. *Про внесення змін до Рішення міської ради №28/5 від 30.03.2016 Про програму інформатизації та інформаційної діяльності Дніпропетровської міської ради на 2016–2020 роки : Рішення Дніпропетровської міської Ради №29/16 від 01.12.2016 року. – [Електронний ресурс]. – Режим доступу : https://dniprorada.gov.ua/upload/editor/29-16.pdf.*
3. *Про захист інформації в інформаційно-телекомунікаційних системах : Закон України № 80/94-ВР від 05.07.1994 року // Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.*
4. *Про інформацію : Закон України № 2657-XII від 02.10.1992 // Відомості Верховної Ради України (ВВР). – 1992 – № 48, ст. 650. – [Електронний ресурс]. – Режим доступ : http://zakon2.rada.gov.ua/laws/show/2657-12.*
5. *Про місцеве самоврядування: Закон України № 280/97 від 21.05.1997 -ВР // Відомості Верховної Ради України. – 1997. – №24. – ст. 170. – [Електронний ресурс]. – режим доступу : http://zakon3.rada.gov.ua/laws/show/ru/280/97-%D0%B2%D1%80/page.*
6. *Про Національну програму інформатизації : Закон України № 74/98-ВР від 04.02.1998 р. // Відомості Верховної Ради України. – 1998. – № 27–28. – ст.181. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.*
7. *Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України № 96/2016 від 15.03.2016 року // Урядовий кур'єр від 18.03.2016№ 52. – [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/96/2016.*
8. *Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security. – [Internet resource] – Access mode. – http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216%2802%29.*

Стаття надійшла до редакції 10.03.2017.