

УДК 342.9

Н.А. Литвин,
кандидат юридичних наук, доцент,
старший науковий співробітник, доцент Університету
державної фіскальної служби України, м. Ірпінь, Київська обл.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У науковій статті досліджено окремі питання правового регулювання інформаційної безпеки України. Проаналізовано стан нормативно-правового регулювання інформаційної безпеки держави, визначено напрями державної інформаційної політики щодо інформаційної безпеки та зроблено висновок щодо врегулювання цієї проблеми.

Порівнюється зміст доктрин інформаційної безпеки України 2009 та 2017 років та наголошується на необхідності імплементації визначених у новій доктрині завдань у практичну площину, тобто створення низки нових нормативно-правових актів у зазначеній сфері.

Ключові слова: інформація, інформаційна безпека, Державна інформаційна політика, інформаційне забезпечення, нормативно-правові акти.

В научной статье исследованы отдельные вопросы правового регулирования информационной безопасности Украины. Проанализировано состояние нормативно-правового регулирования информационной безопасности государства, определены направления государственной информационной политики относительно информационной безопасности и сделан вывод относительно урегулирования данной проблемы.

Сравнивается содержание доктрин информационной безопасности Украины 2009 и 2017 и подчеркивается необходимость имплементации определенных в новой доктрине задач в практическую плоскость, то есть создания ряда новых нормативно-правовых актов в указанной сфере.

Ключевые слова: информация, информационная безопасность, Государственная информационная политика, информационное обеспечение, нормативно-правовые акты.

In the paper, certain issues of legal regulation of information security of Ukraine are investigated. The condition of normative and legal regulation of information security of the state, certain directions of the state information policy regarding information security are analyzed and the conclusion is made regarding the settlement of this problem.

The content of the information security doctrines of Ukraine 2009 and 2017 is compared and the need to implement the tasks defined in the new doctrine into the practical plane, that is, the creation of a number of new regulatory and legal acts in this sphere, is emphasized.

Keywords: information, informative safety, public informative policy, informative providing, normative legal acts.

На сьогодні інформація є одним із головних елементів у багатьох сферах державного управління і важливим фактором суспільних відносин. Зміни, що відбуваються на сучасному етапі в Україні, в першу чергу, пов'язані зі збільшенням

великих обсягів інформації та її швидкою зміною. Тому саме на державу покладається завдання щодо забезпечення доступу громадян України до об'єктивної інформації, пов'язаної з усіма сферами життєдіяльності громадянина, в тому числі інформації, що стосується діяльності органів державної влади. Відповідно, для ефективної діяльності зазначених органів та для забезпечення доступу громадян до якісної інформації важливе місце посідають питання інформаційної безпеки. Адже інформаційна безпека є частиною національної безпеки держави, яка має захищати фінансово-економічну, соціальну, політичну й інші сфери діяльності держави.

Проблемні питання інформаційної безпеки стали предметом наукових розробок у роботах таких вчених, як І. Арістової, І. Березовської, В. Голубєва, В. Гурковського, О. Дзьобаня, Р. Калюжного, В. Конаха, Б. Кормича, В. Ліпкана, Ю. Максименка, А. Марущака, О. Олійника, В. Цимбалюка, О. Юдіна, Р. Юсупова, А. Шапки та ін. Але незважаючи на це, на сьогодні проблеми правового регулювання інформаційної безпеки України потребують додаткового вивчення.

Метою статті є визначення проблемних питань правового регулювання інформаційної безпеки України та надання пропозицій для покращення діяльності із забезпечення інформаційної безпеки країни.

Необхідно вказати на те, що державна політика щодо розвитку та формування інформаційного суспільства повинна:

- забезпечувати доступ громадян до інформації;
- створювати національні системи і мережі інформації;
- зміцнювати матеріально-технічні, фінансові, організаційні, правові і наукові основи інформаційної діяльності;
- забезпечувати ефективне використання інформації;
- сприяти постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- створювати загальні системи охорони інформації;
- сприяти міжнародному співробітництву в галузі інформації і гарантувати інформаційний суверенітет України [1].

Але, на жаль, на сьогодні більшість громадян з недовірою ставляться до державної влади в питаннях отримання інформації. Тому потрібно погодитися із думкою Войцих Н., яка зазначає, що вістря державної інформаційної політики має бути, перш за все, спрямоване на усунення “дефіциту довіри до влади”, який перешкоджає просуванню шляхом реформ. У цьому сенсі ключовим завданням є створення відкритого інформаційного середовища, включаючи забезпечення інформаційної прозорості державної влади, необхідної для формування громадянського суспільства і досягнення взаємодії між суспільством і владою на принципах довіри, взаєморозуміння та ділового партнерства [2, с. 11–12].

Водночас на рівні практичної реалізації інформаційна політика держави в сучасній Україні відзначається різноспрямованістю та нескоординованістю діяльності різних відомств, непослідовністю та непрозорістю в реалізації намічених заходів. Як наслідок – Україна поки що не належить до інформаційно незалежних держав, а її інформаційну сферу характеризують такі ознаки:

- малоефективна система державного регулювання національного медіа-простору, відсутність консолідованого бачення напрямів його подальшого розвитку, нерозвиненість культурних індустрій, національної системи збирання та поширення інформації у глобальному масштабі;
- низький рівень присутності в глобальному медіа-просторі, висока інформаційна залежність від іноземних держав та медіа-структур;

– за наявності позитивної динаміки впровадження телекомунікаційних мереж та комп'ютеризації – ринкова стихійність цих процесів, низька керованість ними з боку держави; збереження відставання у сфері ІКТ, неврегульованість підготовки та працевлаштування в межах держави ІТ-спеціалістів [3].

Крім того, на сьогодні ми можемо констатувати, що існуюче вітчизняне законодавство про інформацію у світлі євроінтеграційних процесів є досить недосконалим, що тягне за собою відсутність системних державно-управлінських рішень, спрямованих на забезпечення захисту стратегічних національних інтересів в інформаційній сфері та породжує недооцінку значення інформаційно-комунікаційного аспекту в процесі розбудови держави, консолідації суспільства, європейської та євроатлантичної інтеграції. Відповідно, зазначене вище дає підстави стверджувати, що значна кількість інформаційної продукції в національному інформаційному просторі не відповідає вимогам чинного законодавства у сфері захисту суспільної моралі, руйнує систему людських цінностей та призводить до деградації суспільства. Це стосується і відносин, пов'язаних із забезпеченням інформаційної безпеки, як найважливіших сьогодні для суспільства та держави, що вимагають найшвидшого законодавчого регулювання.

На жаль, зараз Україна є інформаційно залежною від зарубіжних країн та зарубіжних інформаційних структур, що негативно впливає на стан захисту інформаційних ресурсів, адже зі зростанням значення інформації в суспільному житті, з активізацією глобальних впливів на нації і держави набуває актуальності проблема збереження і постійного оновлення їхнього національного інформаційного простору. Під час інформаційної агресії він є об'єктом першочергового ураження і предметом організації захисту сторони, що зазнала інформаційної агресії з метою унеможливлення маніпулювання громадською думкою, зокрема шляхом поширення недостовірної, неповної та упередженої інформації.

У цьому сенсі державна інформаційна політика повинна відбивати нагальні питання, що склалися в міжнародній сфері та сфері інформаційної безпеки, та базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційної діяльності в національному інформаційному просторі, недопущенні втручання у зміст та внутрішню організацію інформаційних процесів, збереженні та вдосконаленні вітчизняного національного інформаційного продукту та інформаційних технологій, забезпеченні інформаційної ідентифікації України у світовому інформаційному просторі, гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій, сприянні вітчизняному виробництву засобів захисту інформації, створенні захищених інформаційно-телекомунікаційних систем, запровадженні сучасних захищених інформаційних технологій в інтересах державного управління.

Крім того, потрібно вказати на те, що державна інформаційна політика повинна бути направлена на створення ефективної системи виявлення та запобігання загрозам державних електронних інформаційних ресурсів, у тому числі щодо протидії розповсюдженню комп'ютерних вірусів, програмних і апаратних закладок, а також витоку інформації технічними каналами та за рахунок несанкціонованих дій; забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема, шляхом протидії комп'ютерним злочинам; забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та органів місцевого самоврядування, інформаційно-телекому-

нікаційних систем, які функціонують в інтересах управління державою, задовольняють потреби оборони та безпеки держави, кредитно-банківських та інших сфер національної економіки, систем управління об'єктами критичної інфраструктури; удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема кібернетичної безпеки національної критичної інфраструктури; впровадження захищеного механізму ідентифікації учасників електронної взаємодії; формування системи моніторингу безпеки інформаційних ресурсів та систем [4].

На виконання зазначених вище напрямів державою були прийняті нові закони та внесено низку змін до чинних нормативно-правових актів, що регулюють питання інформаційної безпеки, зокрема, Концепції Національної програми інформатизації (1998 р.), Доктрини інформаційної безпеки України (2009 р.), законів України: “Про інформацію” (1992 р.), “Про захист інформації в інформаційно-телекомунікаційних системах” (1994 р.), “Про державну таємницю” (1994 р.), “Про захист інформації в інформаційно-телекомунікаційних системах” (1994 р.), “Про інформаційні агентства” (1995 р.), “Про телекомунікації” (2003 р.), “Про основи національної безпеки України” (2003 р.) “Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” (2007 р.), “Про захист персональних даних” (2010 р.) та ін.

На скільки Україна була не захищена, інформаційно з'ясувалося лише після анексії Криму і початку війни на Донбасі. Саме після цих подій Указом Президента України було прийняте рішення Ради національної безпеки і оборони України “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”. Цей законодавчий акт передбачає у місячний термін внести на розгляд Верховної Ради законопроекти щодо протидії інформаційній агресії іноземних держав, а також розробити механізм протидії негативному інформаційному впливу. У тримісячний термін було запропоновано створити проект нової редакції національної доктрини інформаційної безпеки, проект закону України “Про кібернетичну безпеку України”, проект змін до законів України “Про основи національної безпеки України”, “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про службу безпеки України”, “Про службу спеціального зв'язку та захисту інформації України”. Незважаючи на те, що ці закони переважно були розроблені та впроваджені, технічні можливості нашої держави знаходяться не в найкращому стані. Тому повноцінне функціонування цих же законів, на думку Горбаня Б., подекуди є неможливим. Крім того, необхідно погодитись з його баченням щодо звернення уваги на досвід США та держав-членів ЄС щодо ефективного створення інформаційного законодавства, проте для об'єктивної оцінки фактів варто не забувати, що всі ці країни мають більш ефективну систему технологій.

На сьогодні у США надзвичайно важливе питання – це національна безпека. Ураховуючи особливості сучасного світу, воно включає в себе прогнозування міжнародних відносин; національні доктрини та стратегії національної безпеки; військові стратегії та прогнозування, забезпечення інформаційної безпеки. Усі ці структурні елементи взаємопов'язані. Незважаючи на те, що США мають надзвичайну потужну як юридичну, так і технічну базу, у 2016 році виник скандал (розслідування котрого триває до сьогодні), де очільники Національної розвідки та Міністерства національної безпеки звинуватили Росію у втручанні в перебіг президентських виборів методом злому серверів Демократичної партії США. Країни-члени Європейського союзу ще в 1990-х ухвалили правове підґрунтя забезпечення інформаційної безпеки як у всьому Альянсі, так і в кожній державі окремо. Першочерговими завданнями було визначено: захищати загальні цінності,

основні інтереси та незалежність Союзу; зміцнювати безпеку Союзу та держав-членів усіма способами; розвивати та консолідувати демократію й законність, повагу до прав людини й основних свобод. Ці функції не втратили своєї важливості і сьогодні. Водночас розслідування німецькими спецслужбами дій російських хакерів та ЗМІ продемонструвало, що Москва послідовно провадить інформаційну політику, яка має на меті дестабілізацію політичного клімату в ФРН. Аналогічна ситуація була засвідчена в інших європейських державах. У зв'язку з цим, Європейський союз змушений був осучаснювати своє законодавство щодо інформаційної безпеки. У 2016 році Європейський парламент ухвалив план забезпечення нової Стратегії європейської політики безпеки і оборони. Згідно з цим актом організаторами інформаційних атак Росії на Європу є МЗС Росії та Федеральне агентство “Россотрудничество”, які застосовують у своїй злочинній діяльності комплексні заходи, величезний перелік інструментів, включаючи засоби масової інформації, інформаційно-аналітичні центри та спеціальні фонди. За словами європейських експертів, найбільшу загрозу з них для Європейського Союзу становлять російські пропагандистські агентства, зокрема: агентство “Спутник”, телеканал “Russia Today” та фонд “Русский мир” [5].

Отже, як бачимо, приклади інформаційної безпеки зазначених країн можуть бути корисними для використання основних елементів у законодавстві нашої країни, тим більше коли до сьогодні Росія активно веде гібридну війну проти України та намагається вплинути на значну кількість інших держав. Тому перед урядом України наразі існує потреба в удосконаленні державної інформаційної політики через державно-правове регулювання науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, та ефективно захищала власні національні інтереси.

Говорячи про інформаційну безпеку, доцільно було б зупинитися саме на змісті Доктрини інформаційної безпеки України 2009 року. Олійник О.В. зазначає, що ця доктрина не дає повного уявлення про сукупність офіційних поглядів, цільових настанов, керівних принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз. Доктрина не визначає важливі аспекти забезпечення інформаційної безпеки України, а саме: функції щодо реалізації державної політики у цій важливій складовій забезпечення національної безпеки; організаційну структуру державних органів, інших суб'єктів та їх повноваження щодо реалізації державної політики у цій сфері; порядок координації діяльності суб'єктів з питань забезпечення інформаційної безпеки особи, суспільства і держави. Документ не визначає загроз життєво важливим інтересам і напрямам діяльності, спрямованим на підготовку сил і засобів для активних дій у процесі можливих інформаційних протистоянь із супротивниками і конкурентами, попередження інформаційної агресії та застосування проти України інформаційної зброї та інших негативних інформаційних впливів. Доктриною передбачено забезпечення інформаційної безпеки України лише через засади, заходи і засоби власне інформаційної сфери, тобто сфери обігу інформації і діяльності ЗМІ. Засади державної політики в цій важливій сфері слугуватимуть основою для розробки і впровадження стратегій, доктрин, програм, планів забезпечення інформаційної безпеки на відповідних напрямках життєдіяльності особи, суспільства, держави [6, с. 64].

Тому на реалізацію зазначених недоліків Указом Президента України від 25 лютого 2017 року № 47/2017 рішенням Ради національної безпеки і оборони

України була введена в дію нова Доктрина інформаційної безпеки України. Зазначений нормативний акт є помітним кроком вперед у діяльності держави щодо забезпечення інформаційної безпеки держави та протидії, в першу чергу, російській інформаційній агресії.

Порівнюючи зміст нової Доктрини інформаційної безпеки України із попередньою від 2009 року, ми можемо побачити відчутну різницю. Так, Попова Т. визнає, що головним досягненням є спроба визначити та гармонізувати повноваження органів влади, силових структур щодо їхньої діяльності із захисту інтересів суспільства і держави в інформаційній сфері, національного інформаційного простору. Вона зазначає, що заслуговує уваги нормативне визначення низки термінів. Зокрема, фактично розмежована проблематика урядових комунікацій та стратегічних комунікацій. Зазначене дозволить позбутися певного дублювання та сконцентрувати проблематику стратегічних комунікацій переважно в контексті діяльності сектору безпеки та оборони держави. Крім того, в нормативному акті закріплено термін “наратив”, який є одним із ключових у діяльності суб’єктів забезпечення інформаційної безпеки [7].

Для того, щоб зазначена доктрина запрацювала і повністю реалізувала свою мету, оскільки вона не є нормативним актом прямої дії, що регулює виключно всі аспекти діяльності щодо забезпечення інформаційної безпеки, потрібно щоб державні структури попрацювали над імплементацією визначених у Доктрині завдань у практичну площину, тобто потрібно буде створити низку нових нормативно-правових актів у зазначеній сфері. Це є важливим моментом, оскільки Доктрина окреслює стратегічні питання, а центральні органи виконавчої влади, структури сектору безпеки та оборони мають деталізувати та конкретизувати її вимоги в інших нормативних документах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію: Закон України від 2 жовтня 1992 р. Відомості Верховної Ради України. 1992. № 48. Ст. 651.
2. *Войцук Н.* Державна політика в Українському інформаційному просторі: стан та проблеми. Український інформаційний простір: Науковий журнал Інституту журналістики і міжнародних відносин Київського національного університету культури і мистецтв. Число 1. У 2-х ч. Ч. 2. Київ: КНУКІМ, 2013. С. 10–14.
3. *Гнатюк С.* Актуальні проблеми державної інформаційної політики в Україні. URL: <http://old.niss.gov.ua/monitor/april08/3.htm> (дата звернення 03.07.2017).
4. Офіційний сайт Державного агентства з питань електронного урядування України. URL: <http://www.dknii.gov.ua/content/informaciyna-bezpeka> (дата звернення 05.07.2017).
5. *Горбань Б.* Інформаційна безпека держави в сучасному світі. URL: Режим доступу <https://uain.press/blogs/bogdan-gorban-informatsijna-bezpeka-derzhavy-v-suchasnomu-sviti/> (дата звернення 10.07.2017).
6. *Олійник О.В.* Стан забезпечення інформаційної безпеки в Україні. Юридичний вісник. 2014. № 2(31). С. 59–65.
7. *Попова Т.* Що означає “Доктрина інформаційної безпеки України”? URL: <https://www.radiosvoboda.org/a/28337376.html> (дата звернення 12.07.2017).

Отримано 07.08.2017