Юридичні науки

УДК 342.9

Візір Тетяна Сергіївна

студентка магістратури

Київського міжнародного університету

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ

Анотація. *Досліджено сучасний стан адміністративно-правового регулювання забезпечення інформаційної безпеки в Україні. Виявлено низку проблем у вказаній сфері. Наведено комплекс рекомендацій щодо їх розв'язання. Визначено напрями вдосконалення законодавства, що забезпечує адміністративно-правового регулювання інформаційної безпеки в Україні.*

Ключові слова: *адміністративно-правове регулювання, інформаційна безпека, сучасний стан, перспективи вдосконалення.*

Питання забезпечення інформаційної безпеки та розробки складових державної політики у цій сфері на системному рівні вперше були визначені у рішенні Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України», введеному в дію Указом Президента України від 23 квітня 2008 року № 377/2008, та у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 8 липня 2009 року № 514/2009 (втратила силу на підставі Указу Президента України від 6 червня 2014 року № 504/2014). Водночас вказані напрацювання не були своєчасно реалізовані, а система забезпечення інформаційної безпеки, як засвідчив стан протидії інформаційній агресії РФ,

залишилась неефективною і такою, що не відповідає національним інтересам України.

Аналіз нормативно-правових актів у сфері забезпечення інформаційної безпеки України дозволяє дійти висновку про необхідність удосконалення адміністративно-правового регулювання забезпечення інформаційної безпеки. Адже, норми національного законодавства у вказаній сфері містять чимало прогалин та колізій, мають суперечливий та безсистемний характер.

Питання адміністративно-правового регулювання забезпечення інформаційної безпеки в Україні неодноразово привертало уваги вітчизняних науковців, серед яких: О. В. Олійник, О. Д. Довгань, Ю. П. Лісовська, О.О. Черноног, О. М. Солодка та багато інших.

Однак наявні наукові праці стосуються лише окремих питань даної теми. Крім того, більшість досліджень базуються на застарілих нормах законодавства.

Метою даної наукової статті є оцінка сучасного стану адміністративно-правового регулювання забезпечення інформаційної безпеки в Україні, виявлення проблемних аспектів та шляхів удосконалення законодавства.

Незважаючи на те, що в Україні упродовж останніх років напрацьовано низку законодавчих актів, які регулюють відносини, що виникають в інформаційній сфері, зокрема щодо забезпечення інформаційної безпеки держави, доводиться констатувати, що в сучасних умовах розвитку суспільства інформаційне законодавство потребує якісних змін. За всієї його розгалуженості воно залишається суперечливим, належним чином не систематизованим і не кодифікованим [13, с. 76].

Особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. При чому важливі

проблеми нормативно закріплюються підзаконними нормативно-правовими актами. Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією.

До того ж, Закон України «Про інформацію» не містить визначення поняття «інформаційної безпеки», що є серйозним упущенням вітчизняного законодавця. У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» надається визначення поняття «інформаційна безпека» - це «… стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [21].

Недостатність правового врегулювання правової бази щодо інформаційних правовідносин значно ускладнює настання якісних змін у цій сфері суспільних відносин. На сьогодні у зв'язку з відсутністю взаємопов'язаних, чітко розроблених заходів та теоретичних розробок із забезпечення інформаційної безпеки держави маємо цілу низку перешкод на шляху повноцінної реалізації державою свого обов'язку щодо забезпечення інформаційної безпеки, яка, у свою чергу, є невід'ємною частиною національної безпеки. Лише реалізація науково обґрунтованої державної інформаційної політики може створити ефективну систему протидії правопорушенням у цій сфері [17, с.136-137].

Існування значних недоліків та суперечностей у законодавчій регламентації основних параметрів інформаційної безпеки, протиріччя та прогалини у правозастосовній практиці в цій сфері ускладнюють процес

впровадження у життєдіяльність нашого суспільства правових норм та інституцій, притаманних сучасному цивілізованому світу [16, с. 66].

Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки. Крім того, наявність численних бланкетних чи відсильних норм права, багатьох абстрактних, суб'єктивних понять, що потребують офіційного тлумачення чи чіткого визначення, а також відсутність закріплення фундаментальних, базових дефініцій (наприклад, інформаційна безпека) є джерелами загроз інформаційній безпеці України [17, с. 133].

Проблема забезпечення національних інтересів і національної безпеки в інформаційній сфері поки перебуває на стадії розроблення. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері [17, с. 133-134].

Указом Президента України від 25 лютого 2017 року № 47/2017 було введено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Варто зазначити, що попри свою певну прогресивність вказана Доктрина не позбавлена недоліків. Так, наприклад, метою Доктрини задекларовано «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни». Але, на думку Експерта зі стратегічних комунікацій ГО «Інформаційна безпека» Т. Попової, така мета більше підходить до іншого документа, який має визначати основні засади державної інформаційної

політики, особливо її структуру та зміст. Поки що такого документа на державному рівні в Україні не існує.

Також в експертному середовищі залишаються відкритими питання щодо методології підходів до проблематики забезпечення інформаційної безпеки, які закріплені в Доктрині. На перше місце слід поставити співвідношення понять «інформаційна безпека» та «кібербезпека». Українська наука чітко обґрунтувала необхідність розгляду національного сегменту кіберпростору як складової частини інформаційного простору держави. З цього випливає і логічність розгляду питань кібербезпеки в контексті інформаційної безпеки. Але, враховуючи те, що в Україні державні діячі чомусь соромляться вітчизняної науки, то звернемося до підходів західних країн. Зокрема, в аналітичній доповіді «Information Warfare Boundaries for anArmy in a Wireless World» від корпорації «РЕНД» на замовлення сухопутних військ (армії) ЗС США (звіт 2013 року, код звіту по проекту - RAND10473) зазначено, що в практичній діяльності органів військового управління, суб'єктів забезпечення інформаційної безпеки інформаційне середовище необхідно розглядати як єдине середовище в двох вимірах: людському та технічному. Розгляд інформаційного середовища та кіберсередовища (та, відповідно інформаційної безпеки та кібербезпеки) як окремих паралельних інституцій (напрямів діяльності) визнано необґрунтованим та штучним (тобто визнано методологічною помилкою).

На жаль, в діяльності українських державних структур відбулося штучне відокремлення інформаційної безпеки та кібербезпеки, що відображено в низці нормативно-правових актів. Розбалансованість та розпорошеність діяльності, інституційна невизначеність при таких підходах є чинником зменшення ефективності заходів інформаційного протиборства з боку України.

З інформованих джерел в державних структурах неодноразово можна було почути інформацію про те, що ціла низка пропозицій до змісту

Доктрини, змін та доповнень з боку силових структур, незалежних експертів, наукових установ не були взяті до уваги. Тому навіть на засідання Ради нацбезпеки та оборони, на якому мав розглядатися проект Доктрини, деякі члени РНБОУ прибули з ґрунтовними тезами щодо необхідності відправити Доктрину на доопрацювання.

Існує кілька ризиків щодо успіху реалізації положень Доктрини. Перш за все, історичною рисою українських органів влади є невідповідність між рівнем нормативного регулювання того чи іншого напряму їх діяльності та реальними кроками щодо виконання ними положень правових актів. Щоб не допустити повторення цієї тенденції стосовно Доктрини, держструктурам доведеться все ж таки попрацювати над імплементацією визначених завдань у практичну площину.

В цьому контексті доведеться дуже ретельно попрацювати над новими нормативно-правовими актами. Слід бути відвертими - Доктрина не є нормативним актом прямої дії, що регулює виключно всі аспекти діяльності щодо забезпечення інформаційної безпеки. Вона окреслює стратегічні питання, а центральні органи виконавчої влади, структури сектору безпеки та оборони мають деталізувати та конкретизувати її вимоги в інших нормативних документах.

Іншим ризиком є відсутність реально працюючих механізмів координації діяльності в сфері інформаційної безпеки. Деякі успішні приклади горизонтальної взаємодії органів влади, волонтерські проекти, проекти у форматі «ручного управління» - є виключенням із правил, які лише підтверджують необхідність офіційної координації з боку держави. Безумовно, необхідність централізації діяльності, дієвих алгоритмів координації та контролю в тексті Доктрини задекларовані. Але, з іншого боку, механізми зазначеного не прописані. РНБОУ отримало завдання координації діяльності, не маючи при цьому необхідних повноважень та ресурсів, які притаманні центральним органам виконавчої влади.

Мінінформполітики в існуючому вигляді також не зможе виконати певні завдання, не будучи до того ж офіційною складовою частиною сектору безпеки та оборони держави та суб'єктом боротьби з тероризмом.

І якщо Мінінформполітики серед інших міністерств та відомств виконавчої влади визнано фактично головним суб'єктом забезпечення інформаційної безпеки, то це накладає певні зобов'язання. Особливо щодо проблематики активних заходів інформаційного впливу, необхідності координації діяльності силових структур, які, між іншим, зобов'язані займатися такими заходами, як інформаційні та психологічні операції. Тобто на порядку денному - перезавантаження Мінінформполітики. Втім, на жаль, наразі не можна стверджувати, що на таке перезавантаження вистачить політичної волі, професіоналізму та кадрового ресурсу.

Слабким місцем Доктрини також є недостатнє правове регулювання максимально можливого залучення громадянського суспільства до заходів забезпечення інформаційної безпеки. Такі громадські проекти, як «СтопФейк», «Інформнапалм» де-факто існують та ефективно діють. А в нормативному плані таких проектів ніби то й нема, їхня співпраця з державою практично не регламентована [19].

Важливою проблемою залишається певна несистемність вітчизняної правової політики в інформаційній сфері. Значна кількість законодавчих актів ухвалюється з метою вирішення певних тактичних завдань, задоволення кланових інтересів, часто без урахування стратегічних орієнтирів та реальних українських умов. Показовим з цієї точки зору є неодноразові спроби перегляду законодавства щодо дозволу рекламування алкоголю і тютюну. Значним недоліком чинного законодавства, зокрема в інформаційній сфері, є його неконкретність, певна розмитість формулювань. Фактично відсутні визначення конкретних механізмів оприлюднення інформації, конкретних документів, що мають

публікуватися. Не встановлюються терміни цієї діяльності, майже відсутні норми прямої дії щодо фінансового та кадрового забезпечення.

Левова частка інформаційних відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Характерним прикладом останнього є відсутність законодавчого визначення режимів доступу до інформації, окрім державної таємниці. Незважаючи на те, що в законодавстві існують поняття комерційної, лікарської, банківської таємниці, інформації «не для друку» тощо, їхнє чітке визначення відсутнє. Режим доступу до інформації, що належить державі, чомусь встановлюється постановами Кабінету Міністрів України.

Хоча основи інформаційного законодавства України у сфері інформаційної безпеки вже є, нині чинна законодавча база потребує подальшого розвитку та вдосконалення з багатьох аспектів у відповідних законах і Доктрині інформаційної безпеки України. При цьому забезпечення інформаційного суверенітету та гарантування інформаційної безпеки України з правової точки зору повинно включати:

– визначення та уніфікацію загальних положень законодавства;

– засад і норм регулювання інформаційних відносин у різних галузях суспільної діяльності та сферах національної безпеки;

– визначення та забезпечення державою стратегічних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;

– визначення норм, засад і меж діяльності вітчизняних і зарубіжних суб'єктів інформаційних відносин у національному інформаційному просторі України;

– визначення засад, принципів, методів щодо захисту національних інтересів України як у вітчизняному, так і в світовому інформаційному просторі та міжнародних інформаційних відносинах [9, с.134-135].

Аналіз аспектів розвитку інформаційного суспільства, інформаційної глобалізації та інформаційного протистояння в сучасних умовах загалом засвідчив наявність низки проблем організаційно-правового змісту у сфері інформаційної безпеки України, а саме:

– недосконаліть державної політики з питань інформаційної безпеки;

– відсутність стратегічного рівня забезпечення інформаційної безпеки;

– неналежний рівень інформаційного супроводження зовнішньої та внутрішньої політики України;

– відомчу автономність державних органів та установ, на які покладено завдання забезпечення інформаційної безпеки України, дублювання їх повноважень та недостатня якість наявної координаційної складової;

– відсутність дієвих механізмів експертної оцінки інформаційної продукції, поширення якої створює загрозу інформаційній безпеці щодо прав людини, інтересам суспільства та держави;

– відсутність ефективних механізмів залучення громадськості та приватного сектору України до протидії негативним інформаційним впливам, міжнародної співпраці у цій сфері;

– наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом [23, с.38].

Для України сьогодні логічним кроком на шляху до інформаційного майбутнього є розробка цілісної гнучкої динамічної державної політики інформаційної безпеки, яка враховуватиме багатоаспектність явища інформаційної безпеки, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення в суспільній свідомості, а також на

правовому концептуально-доктринальному рівні та на рівні ефективного і зручного (систематизованого) інформаційного законодавства [10, с.178].

Потребує вдосконалення національне законодавство й у частині регулювання забезпечення кібербезпеки. Аналіз правових засад адміністративно-правового регулювання кібербезпеки дозволяє встановити низку недоліків у цій сфері, серед яких:

- відсутність узгодження понятійного апарату у сфері адміністративно-правового регулювання кібербезпеки в Україні, зокрема, відсутність чіткого визначення, змісту та сутності категорій, що призводить до їх неоднозначного розуміння та застосування, що, у свою чергу, створює умови для уникнення відповідальності правопорушників;
- штучне розширення предмету інформаційної безпеки на максимальну кількість сфер, що розмиває сам предмет інформаційної безпеки, а також обумовлює відсутність частини «кібер» у вітчизняних нормативно-правових документах [24];
- надмірна розпорошеність адміністративно-правових норм, що стосуються кібербезпеки в Україні. Значна кількість адміністративно-правових норм щодо адміністративно-правового регулювання кібербезпеки в Україні міститься в різних нормативно-правових актах, що ускладнює пошук, аналіз та узгодження для практичного застосування;
- неузгодженість нормативно-правових актів, норми яких регламентують адміністративно-правове регулювання кібербезпеки в Україні, як між собою, так і з чинною Конституцією України;
- побічне згадування кібербезпеки в стратегічних документах забезпечення воєнного сектору;
- декларативність значного масиву норм без указівок на шляхи їх реалізації, унаслідок чого спостерігається низький рівень правореалізації норм, що регулюють суспільні відносини у сфері забезпечення та організації кібербезпеки тощо.

У свою чергу, недосконаліть національного законодавства у сфері адміністративно-правового забезпечення та організації кібербезпеки України значно підвищує ймовірність реалізації кіберзагроз, що негативно впливає на загальний рівень національної безпеки України. Це викликає необхідність:

- прискорення адаптації до європейських правових норм і стандартів;
- забезпечення належної координації дій усіх заінтересованих суб'єктів під час запровадження інструментів забезпечення та організації кібербезпеки;
- удосконалення інституціонального механізму формування, координації та здійснення контролю за виконанням завдань розбудови кібернетичного суспільства;
- підвищення рівня представленості України в кіберпросторі та присутності в ньому українських інформаційних ресурсів;
- забезпечення прийняття системних державних рішень, спрямованих на стимулювання створення національних інноваційних структур (центрів, наукових парків і технопарків) для розроблення конкурентоспроможних вітчизняних інформаційно-комунікаційних технологій;
- підвищення на державному рівні значущості українського сегмента кіберпростору, як одного з найважливіших інструментів розвитку інформаційного суспільства та конкурентоспроможності держави;
- розробки на національному та місцевому рівні механізм ефективної громадської участі та громадського контролю за реалізацією пріоритету розбудови інформаційного суспільства [4, с.122].

Крім того, для оперативної та ефективної протидії кіберзлочинності суттєвим питанням є розробка та внесення в установленому порядку на розгляд Верховної Ради України законопроектів щодо імплементації

положень Конвенції про кіберзлочинність, ратифікованої Законом України від 07 вересня 2005 року № 2824-IV [7], передбачивши, зокрема:

1) надання правоохоронним органам повноважень щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних (операторам і провайдерам телекомунікацій, іншим юридичним і фізичним особам) про термінове фіксування та зберігання комп'ютерних даних, необхідних для розкриття злочину, на строк до 90 днів із можливістю продовження такого строку до 3-х років, а також унормування порядку внесення зазначених приписів;

2) установлення вимог щодо надання операторам і провайдерам телекомунікацій на вимогу правоохоронних органів інформації, необхідної для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

3) запровадження блокування (обмеження) за рішенням суду операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу);

4) запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі здійснення оперативно-розшукової діяльності.

Крім того, в умовах виникнення нових загроз національній і міжнародній безпеці, повсякденного зростання кількості та потужності кібератак на державні й фінансові установи, вмотивованих інтересами окремих держав, груп та осіб, постала необхідність затвердити протокол спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак і кіберінцидентів, а також при усуненні їхніх наслідків.

Також існує нагальна потреба в прийнятті єдиного комплексного системоутворюючого законодавчого акта, який би забезпечив створення

єдиної стратегії реалізації державної політики у сфері кібербезпеки; розроблення організаційно-правових механізмів забезпечення кібербезпеки; визначення правового статусу суб'єктів відносин у сфері адміністративно-правового регулювання кібербезпеки, установлення їх відповідальності за дотримання національного законодавства у цій сфері; створення системи підготовки кадрів, які використовуються в галузі кібербезпеки. Таким вимогам, на думку науковців, відповідає проект Закону України «Про основні засади забезпечення кібербезпеки України [4, с. 122].

Протидії кіберзлочинності також сприятиме розробка спеціального Закону про боротьбу з кіберзлочинністю. Так, заслуговує на увагу Проект Закону «Про основні засади забезпечення кібербезпеки України» № 2126а від 19 червня 2015 р. [19], спрямований на правове регулювання та розбудову захищеного інформаційного простору держави, прогресивного розвитку ІТ-сфери, як рушійної сили становлення безпекового цифрового суспільства та цифрової економіки України, які є невід'ємними умовами входження в європейський інформаційний простір. Суттєвою перевагою та досягненням законопроекту є закріплення понятійного апарату, а саме таких понять, як кібератака, кібербезпека, кіберзагроза, кіберпростір, кіберзлочин та інші, визначення суб'єктів національної системи кібербезпеки та їх завдань. Вказаний законопроект викликав інтерес та критику з боку науковців і практиків. Одним із суттєвих недоліків документу є те, що встановлені завдання суб'єктів національної системи кібербезпеки не узгоджуються з базовими чинними законодавчими актами, які регулюють діяльність таких органів, залишається невизначеним, хто буде відповідати за забезпечення кібербезпеки в інших сегментах, зокрема: органів державної влади та державного управління, економіки, судової системи, приватного сектору. Згідно з висновком Інтернет-асоціації України, виходячи зі змісту статті 9 проекту Закону, залишається невизначеним, який державний орган

у повному обсязі матиме повноваження щодо формування державної політики задля забезпечення кібербезпеки України.

Крім того, в проекті Закону «Про основні засади забезпечення кібербезпеки України» [19] запропоновано визначення суб'єктів забезпечення кібербезпеки постійної готовності: державні органи або їх підрозділи, що входять до складу національної системи кібербезпеки, сили та засоби яких спеціально виділені для перебування в постійній готовності до реагування на кіберзагрози та оперативного виконання завдань забезпечення кібербезпеки. Відповідно до положень ст. 8 проекту національну систему кібербезпеки складають РНБО, Міністерство оборони України, Генеральний штаб Збройних Сил України Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Міністерство внутрішніх справ (на відміну від Національної поліції України як зазначено в прийнятій Стратегії [22]), розвідувальні органи. Один із суб'єктів національної системи кібербезпеки, визначений Стратегією кібербезпеки - Національний банк України - в законопроекті не вказується. У цілому позитивно оцінюючи проаналізований законопроект, доцільним є приведення його у відповідність до прийнятих стратегічних документів.

Аналіз антиукраїнських дій в інформаційному просторі вказує на те, що слід зробити акцент на збереженні національної ідентичності та популяризації національної культури як базису не лише інформаційної безпеки України, але й загалом національної. Захист інформаційного суверенітету України виділяється як один із пріоритетних напрямів забезпечення національної безпеки. Проте законодавство не містить адекватного тлумачення зазначеного поняття, як і конкретних механізмів його забезпечення. Так, на сьогодні взагалі відсутній механізм ефективного та швидкого блокування (обмеження доступу) ресурсів з протиправним контентом, зокрема розміщених на технічних майданчиках за кордоном, як

і власне визначення шкідливого контенту. Окрім цього, відсутній механізм запобігання та протидії поширенню інформаційної продукції антиукраїнського змісту, шляхом визначення загальних критеріїв її віднесення до заборонених для розповсюдження; визначення суб'єкта, який би виконував функцію експертного оцінювання інформаційної продукції, що містить заклики до порушення конституційного ладу, територіальної цілісності, пропаганду війни, фашизму, національної та релігійної ворожнечі [23, с. 39].

В нашій країні відсутня ієрархічно побудована організаційна структура державних органів від вищих ланок гілок влади до громадянина з чітким визначенням соціально уповноважених органів, які організують і координують цю діяльність у сфері інформаційної безпеки. Це одна з причин поразки і втрат державної політики України як на міжнародній арені, так і у внутрішніх справах, а також невиконання настанов чинного законодавства [18, с. 63].

В Україні створена система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня - Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів, інших відомчих, нормативних актах. Проте вона є неефективним управлінням діяльності системи забезпечення інформаційної безпеки України, що унеможливлює стійке функціонування центральних органів виконавчої влади, які визначають і реалізують політику в інформаційній сфері. Організаційні зміни в системі органів виконавчої влади, що проводяться в рамках адміністративної реформи, мають несистемний характер. Розподіл функцій між окремими суб'єктами системи та схема їх взаємодії потребують вдосконалення. Відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади значно ускладнює

прийняття ними виважених рішень, породжує конфліктні ситуації у владних структурах і суспільстві [6].

На сьогодні, у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову, хоча з урахуванням практики країн Європейського Союзу, інформаційна безпека повинна бути побудована на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх утримання й забезпечення безпеки на основі принципів демократії, прав людини, захищеного Інтернету тощо. Все це потребує законодавчого закріплення в найкоротший термін, оскільки нормативним актом буде визначено єдиний понятійно-категоріальний апарат, державну політику забезпечення інформаційної безпеки, об'єкти інформаційної безпеки та суб'єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур із іншими органами та відомствами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України, та ін. Прийняття такого нормативного акта, на нашу думку, має задати загальну логіку не лише подальшої нормотворчої діяльності, а й сутнісно сформулювати бачення Україною нових геополітичних умов існування держави передусім щодо її ролі в глобальному та національному інформаційних просторах, стати запорукою вирішення проблем в інформаційній сфері. Крім того, після прийняття такого акта та створення системи забезпечення інформаційної безпеки, на наше переконання, непогано було б провести вивчення реального стану в інформаційній сфері України і за результатами сформувати відповідний документ з визначенням: ступеня розвитку та основних загроз в інформаційній сфері; сил, які потрібно залучити для вирішення завдань протидії виявленим загрозам та негативним сценаріям розвитку; оцінки

наявних можливостей суб'єктів забезпечення інформаційної безпеки щодо протидії виявленим загрозам та негативним сценаріям розвитку; аналізу стану кадрового, фінансового, матеріально-технічного та інших видів їх забезпечення; підходів до формування оптимальної моделі забезпечення інформаційної безпеки з урахуванням реальних можливостей та ресурсів; найбільш перспективних альтернативних моделей та стратегій досягнення поставлених завдань та ін. Це в свою чергу стане джерелом якісного аналізу інформаційної сфери України та своєрідним звітом про ефективність системи забезпечення інформаційної безпеки з урахуванням тих змін, які відбуваються в інформаційному середовищі України [5, с. 15-16].

Існує нагальна проблема недотримання встановлених норм усіма суб'єктами інформаційних відносин, зокрема органами державної влади всіх рівнів. До того ж рівень правової культури громадян України змушує розглядати ситуацію із зовсім іншого боку порівняно з країнами ЄС. Тобто, недостатньо ретельне та чітке дотримання законодавства складає найважливішу проблему правової політики держави, у тому числі це стосується й інформаційної сфери. Показовим, протягом усього періоду існування незалежної України, є намагання певних сил створити новітні зони недоторканості, сформувати потужні системи пільг та переваг, що діють поза законодавством. Забезпечення єдності та невідворотності дії Закону є провідним завданням держави.

Беручи до уваги вище наведене, вважаємо цілком обґрунтованою необхідність розроблення та прийняття Інформаційного кодексу. Як, як доречно зазначає М. Г. Кантока, саме кодифікація вирішить такі проблеми нормативно-правового регулювання інформаційної безпеки України, як розпорошеність, неузгодженість чи неоднозначність нормативно-правових актів у цій сфері [29, с. 62].

Варто вдосконалювати та покращувати механізми співпраці з міжнародними партнерами й організаціями у сфері інформаційної безпеки.

Такий підхід принесе не тільки нові знання та навики, а й дасть змогу оперативно й надійно використовувати міжнародні механізми захисту інформаційної безпеки держави. Потрібно розробити та впровадити в навчальних закладах, підприємствах, установах та організаціях спеціальні державні програми для оволодіння навичками користування інформаційними технологіями, щоб під час використання інформації запобігти виникненню конфліктних ситуацій між інтересами суспільства, держави чи окремих громадян. Окремо забезпечити координацію дій державних і недержавних інституцій у сфері забезпечення інформаційної безпеки [29, с. 62].

На думку В. Негодченко, з метою оптимізації адміністративного законодавства, що регулює різноманітні аспекти захисту національного інформаційного простору від негативних інформаційних впливів, було б доцільно доповнити перелік основних напрямів державної інформаційної політики, закріплених у Законі України «Про інформацію», такими: сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їх забезпечення; розвиток адміністративного законодавства у сфері інформаційних процесів (у тому числі приведення законодавчої бази у відповідність до міжнародних стандартів у цій сфері), інформатизації і захисту інформації; підтримка проектів і програм інформатизації; правове регулювання функціонування в Україні міжнародних інформаційних систем (зокрема, мережі Інтернет); пропагування курсу держави на створення та розвиток відкритого інформаційного суспільства; подальший розвиток інформаційного права як самостійної галузі права та ін. У результаті це дасть змогу підтримати політичний та соціально-економічний курс нашої держави, удосконалити правове регулювання відносин в інформаційній сфері, підвищити ефективність інформаційної культури населення та відповідальне ставлення до користування інформаційним простором; оптимізувати системи

управління інформаційними ресурсами як на загальнодержавному, так і індивідуальному рівні [14, с. 80].

На думку Я. Малик, ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління інформаційною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення, зокрема вдосконалення законодавства з питань національної безпеки, насамперед шляхом:

- розвитку правових засад управління національною безпекою через розробку відповідних законів, концепцій, доктрин, стратегій і програм, зокрема антикорупційного законодавства, Національної програми протидії тероризму та екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;
- розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами, зокрема з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність;
- приведення законодавства з питань охорони державної таємниці до європейських стандартів;
- розробка та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці [11, с. 20].

Важливо також звернути увагу 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 було також встановлено недотримання строків при розробці та прийнятті 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 [24, с. 45].

Захист інформаційної безпеки має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в інформаційній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції [33, с. 146].

У даному контексті слушно заважує О. М. Солодка. На її думку, пріоритетами удосконалення забезпечення інформаційної безпеки є:

– удосконалення правового забезпечення інформаційної безпеки шляхом розробки її концептуальних основ: визначення або уточнення завдань, функцій і повноважень суб'єктів забезпечення інформаційної безпеки України; забезпечення інформаційного суверенітету України з метою недопущення інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур;

– сприяння розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, посиленню міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі;

– зміцнення організаційних основ забезпечення інформаційної безпеки: вирішення питання координації діяльності суб'єктів забезпечення інформаційної безпеки, зокрема у сфері протидії інформаційній агресії, забезпечення кібернетичної безпеки України;

– налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки;

– запровадження системи демократичного контролю за діяльністю державних суб'єктів забезпечення інформаційної безпеки;

– розвиток комунікаційної політики у стосунках «держава-суспільство» [23, с.40-41].

Дещо іншої думки О. Д. Довгань. До пріоритетів забезпечення інформаційної безпеки в Україні автор відносить:

- забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;
- створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
- протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;
- розробка і реалізація скоординованої інформаційної політики органів державної влади;
- виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;
- створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО;
- удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу [19, с.11-12].

Для успішного входження нашої держави в міжнародні інформаційні обміни необхідно зосередитись, насамперед, на таких напрямах у сфері правової діяльності:

– розробка системи правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток і ефективне використання в національних інтересах;

– здійснення необхідної адаптації національного інформаційного законодавства до загальновизнаної міжнародної правової бази з метою активізації своєї участі у інформаційних обмінах;

– активна участь у міжнародній правотворчості, що має оперативно регламентувати нові явища в сфері інформатизації;

– формування правової бази для регламентації участі у міжнародній діяльності по забезпеченню дотримання міжнародного інформаційного законодавства, боротьби з кібертероризмом та іншими видами інформаційної злочинності [5].

Водночас погоджуємось з тим, що розроблення національної правової бази, її гармонізація сприятиме зміцненню інформаційної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави.

Викладене вище дозволяє зробити висновок про те, що чинне національне законодавство України у частині адміністративно-правового регулювання сфери інформаційної безпеки України потребує вдосконалення. Насамперед, вбачається за необхідне:

- доповнити Закон України «Про інформацію» визначенням поняття «інформаційної безпеки;

- привести у відповідність нормативно-правові акти України різної юридичної сили, що стосуються сфери інформаційної безпеки;

- внести комплекс змін, доповнень та уточнень до законодавчої бази з різних питань адміністративно-правового регулювання забезпечення інформаційної безпеки України, що наразі не знайшли належного врегулювання;

- привести у відповідність до міжнародних та європейських норм та стандартів вітчизняне законодавство у сфері забезпечення інформаційної безпеки;
- розробити належне правове забезпечення міжнародного співробітництва з питань інформаційної безпеки.

Насамкінець, слід зауважити, що адміністративно-правове регулювання сфери інформаційної безпеки України потребує подальшого наукового дослідження у напрямку пошуку шляхів вдосконалення національного законодавства у даній сфері.

Література

1. Галіцина Н. В. Адміністративно-правові засади процедури створення та функціонування товариств з обмеженою відповідальністю в Україні: автореф. дис. … канд. юрид. наук: спец. 12.00.07 / Н. В. Галіцина; Класич. приват. ун-т. Запоріжжя, 2010. - 20 с.
2. Городецька І. А. Сутність адміністративно-правового регулювання суспільних відносин у галузі охорони, використання і відтворення тваринного світу / І. А. Городецька // Форум права. - 2016. - №1. С. 60-66.
3. Даценко О. М. Адміністративно-правове регулювання нафтогазового комплексу / О. М. Даценко // Visegrad Journal on Human Rights. - 2015. - №5/1. - С. 24-30.
4. Демедюк С. В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні / С. В. Демедюк // Південноукраїнський правничий часопис. - 2015. - №3. - С.119-123.
5. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України / О.Д. Довгань // Інформаційна безпека людини, суспільства, держави. - 2015. - № 3 (19). - С. 6-16.

6. Домбровська С. Механізми забезпечення інформаційної безпеки як складової безпеки України / С. Домбровська // Теорія та практика державного управління. - №1 (48). - 2015. - С.1-5.
7. Конвенція про кіберзлочинність (ратифіковано із застереженнями і заявами Законом № 2824-IV від 07 верес. 2005 р.) [Електронний ресурс]. – Режим доступу: http://zaNon1.rada.gov.ua
8. Конституція України: станом на 25.04.2019 р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80
9. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем / О. В. Левченко // Збірник наукових праць Харківського університету Повітряних Сил. - 2014. - №3(40). - С.130-135.
10. Лісовська Ю. П. Державна політика забезпечення інформаційної безпеки України: адміністративно-правовий аспект / Ю. П. Лісовська // Молодий вчений. - 2015. - № 2(3). - С.177-180.
11. Малик Я. Інформаційна безпека України: стан та перспективи розвитку / Я. Малик // Збірних наукових праць «Ефективність державного управління». - 2015. - №14. - С.13-20.
12. Миронець І. М. Адміністративно-правове регулювання будівельної діяльності в Україні: автореф. дис. … канд. юрид. наук: 12.00.07 / І.М. Миронець; Нац. авіац. ун-т; К., 2012. - 24 с.
13. Мороз Н. С. Законодавче регулювання інформаційної сфери як основа забезпечення інформаційної безпеки держави / Н. С. Мороз // Вісник Національного університету «Львівська політехніка». Юридичні науки. - 2015. - № 824. - С. 71-76.
14. Негодченко В. Основні напрями державно інформаційної політики в Україні / В. Негодченко // Підприємництво, господарство і право. - 2016. - №4. - С.77-81.

15. Нікітін Ю. В. Національна безпека України в сучасних умовах: ризики і фактори впливу / Ю. В. Нікітін // Юридична наука. - 2015. - №2. - С. 141-147.
16. Олійник О. В. Адміністративно-правові засоби забезпечення інформаційної безпеки / О. В. Олійник // Юридичний вісник. - 2015. - №1. С. 65-69.
17. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні / О. В. Олійник // Право і суспільство. - 2012. - №3. - С.132-137.
18. Олійник О. В. Стан забезпечення інформаційної безпеки в Україні / О. В. Олійник // Юридичний вісник. - 2014. - №1. - С.59-65.
19. Попова Т. Що означає «Доктрина інформаційної безпеки України»? [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/28337376.html
20. Про основні засади забезпечення кібербезпеки України: Проект Закону № 2126а від 19 червня 2015 р. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/ zweb2/webproc4_1?pf3511=55657
21. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. // Відомості Верховної Ради України. - 2007. - № 12. - Ст. 102.
22. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу:http://zaNon2.rada.gov.ua/laws/show/96/2016
23. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України / О. М. Солодка // Інформація і право. - 2015. - №3. - С.36-42.
24. Терехов В. Удосконалення адміністративно-правового регулювання реалізації політики інформаційної безпеки в органах місцевого самоврядування / В. Терехов // Актуальні проблеми правознавства. - 2017. - №1. - С.43-47.

25. Черноног О. О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління. [Електронний ресурс]. – Режим доступу: http://mino.esrae.ru/178-1484