УДК 35.746.1

**СОЛОДКА О.М.,** *кандидат юридичних наук, старший науковий співробітник*

# ПРІОРИТЕТИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

***Анотація.*** *В статті розглядаються пріоритети удосконалення інформаційної безпеки України на основі аналізу внутрішніх та зовнішніх чинників, європейських тенденцій та сучасної ситуації в країні.*

***Ключові слова:*** *інформаційна безпека, пріоритети інформаційної безпеки, національні інтереси.*

***Аннотация.*** *В статье рассматриваются приоритеты совершенствования информационной безопасности Украины на основе анализа внутренних и внешних факторов, европейских тенденций и современной ситуации в стране.*

***Ключевые слова:*** *информационная безопасность, приоритеты информационной безопасности, национальные интересы.*

***Summary.*** *The article deals with the priorities of information security improvement based on the analyse of internal and external factors, EU tendencies and current situation in Ukraine.*

***Keywords:*** *information security, the priorities of information security, national interests.*

Постановка проблеми. Динаміка відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені норми суспільних відносин, ускладнює створення стабільної правової регламентації. Недосконаліть нормативно-правової бази дозволяє окремим суб’єктам реалізовувати свої протиправні наміри в інформаційній сфері як щодо життєво важливих інтересів інших суб'єктів, так і об’єктів національної безпеки.

Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері.

Зазначене вище знаходить відображення у прийнятій Стратегії Національної безпеки України [1]. У своїх положеннях вона визначила пріоритети державної політики національної безпеки, вказавши на основні її цілі, а саме: мінімізацію загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави; утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО. Крім того, Стратегія визначила як основні загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Викладене обумовлює актуальність теми дослідження.

*Дослідження останніх публікацій.* Дослідженню різнобічних аспектів інформаційної безпеки присвячені праці значної кількості вітчизняних та зарубіжних науковців: філософських засад становлення інформаційного суспільства як нової постіндустріальної формації – Д. Белла, У. Дайзарда, Е. Тоффлера, Т. Стоуньєра; правових механізмів забезпечення інформаційної безпеки – О.А. Баранова, О.Д. Довганя, Б.А. Кормича, А.І. Марущака Г.В. Новицького, В.Г. Пилипчука, О.О. Тихомирова, В.М. Фурашева, М.Я. Швеця та інших. Проте, незважаючи на значний рівень наукового осмислення проблем інформаційної безпеки, в сучасних умовах стрімкого розвитку інформаційних технологій, засобів та способів ведення інформаційних війн нагальними є питання удосконалення її забезпечення, що й обумовлює актуальність наукової статті.

***Метою статті*** є визначення пріоритетних напрямів удосконалення забезпечення інформаційної безпеки України.

***Виклад основного матеріалу.*** Фактором, що послаблює здатність держави нейтралізувати загрози, є посилення взаємозалежності країн та їх відкритість до зовнішніх впливів. Здебільшого держава перестає бути монополістом на власній території, її інформаційна політика все більш обмежується, корегується, нівелюється діями інших держав, міжнародних та недержавних організацій, неформальних об’єднань негативної спрямованості, кримінальних угруповань тощо. Слабка ідеологічно, інституційно, економічно держава не здатна скористатися технологічними, економічними, соціокультурними перевагами глобалізації, проте активно переймає її негативні риси [2].

Розвиток глобальних процесів на основі всеосяжної інформатизації створює широку різноманітність інформаційних загроз – від витіснення на внутрішньому інформаційному ринку вітчизняних продуктів більш конкурентоспроможними аж до ведення цілеспрямованих інформаційних війн. Згідно з доповіддю Національної ради з розвідки США, інформаційні війни будуть домінантним фактором у нинішньому столітті. Вони вестимуться на всіх рівнях соціальної структури людства між блоками держав включно. Сучасна інформаційна революція розгортається на фоні інформаційних війн, які своєю головною метою ставлять підрив національної безпеки держав. З урахуванням таких підходів безпекова інформаційна функція держави в усіх регіонах світу набуває особливої важливості [3].

Наявна ситуація в світовому інформаційному просторі обумовлена наступним:

- більшість країн світу зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки;
- протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля;
- набувають поширення агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції;
- майже у 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її елементів (для порівняння – розробки зброї масового знищення здійснюються у близько 20 країнах);
- наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України, РФ і США) можуть бути зіставленими із застосуванням зброї масового ураження;
- новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку [4, с. 3-7].

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:

- недосконалість 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.

При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками:

- внутрішні – найбільшою мірою пов’язані з відсталістю інформаційних технологій в Україні від провідних країн світу, низьким рівнем інформатизації, розпорошеністю повноважень органів державної влади та законодавства в інформаційній сфері;
- зовнішні – загальносвітові тенденції створення та застосування інформаційних технологій та намаганнями іноземних суб’єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів, залежність від іноземного програмного забезпечення.

Відтак, на сучасному етапі Україні слід зосередитись на двох основних напрямах:

- зробити внутрішній український простір сучасним, повноструктурним та конкурентоспроможним;
- забезпечити інформаційну присутність держави в світі та просувати її позитивний імідж.

Забезпечення національної безпеки здійснюється за умови пріоритетності національних інтересів, необхідності своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам, і ґрунтується на засадах правової демократичної держави. А оскільки інформаційна безпека є частиною національної, то тут теж повинен бути пріоритет національних інтересів в інформаційній сфері.

Незважаючи на те, що на сьогодні науковцями виділяється дві складових забезпечення інформаційної безпеки – активна і пасивна (розвиток і захист) [5], у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову. Проте, аналіз практики країн ЄС свідчить про те, що 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.

Разом з тим, інформаційна безпека є невід’ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через

нарощування технологічних можливостей інформаційного обміну, але й через її глибоке усвідомлення усіма суб’єктами інформаційних відносин. Як наслідок, до проблем інформаційної безпеки на цьому етапі починають долучатися питання інформаційної етики, забезпечення приватності в умовах інформаційного суспільства, захисту від маніпулятивних інформаційних впливів тощо.

Відтак, основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації (далі – ЗМІ) до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, захист персональних даних, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов’язків, за критику;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [6].

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.

Поряд із поняттям “інформаційний суверенітет” широко вживається “цифровий суверенітет”, яке тісно пов’язане з поняттям “кібервійна”, що є продовженням війни за допомогою інформаційних і комунікаційних систем, проте із двома фундаментальними відмінностями: вона не призводить до фронтального протистояння ворогуючих сторін та прямих жертв [7].

Зважаючи на низку важливих проблем, що заважають створити ефективно діючу національну систему протидії загрозам в кіберпросторі, а саме: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств,

залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів актуальним є питання побудови системи кібернетичної безпеки.

Застарілість, складність системи охорони державної таємниці та службової інформації, створення умов для її несанкціонованого розповсюдження, переважна “паперовість” носіїв такої інформації ставить питання щодо необхідності гармонізації інформаційного законодавства з нормами міжнародного права і правовими актами ЄС, РЄ і НАТО, що перш за все ґрунтується на невід’ємному праві доступу до інформації. І в першу чергу, саме держава має забезпечувати якісний доступ всіх категорій громадян до виробленої нею інформації, як до офіційних матеріалів, так і до роз’яснення змісту своєї власної діяльності.

Окрім цього, аналіз законодавства розвинутих країн вказує на те, що право на доступ до інформації трансформується у право на комунікацію, яке передбачає не лише право на ознайомлення з інформацією, а й право участі у її створенні. Наприклад, замість розуміння публічної інформації як такої, що “надсилається” з політичної організації або державного органу громадянам, у Норвегії її розглядають як спільно вироблену та використану з громадянами, а також групами громадян самостійно, у спосіб активних інноваційних практик відтворення різних видів доступної інформації, урядової чи ні, у нові форми публічної інформації. Водночас доступ до “старої” публічної інформації має бути настільки відкритим, наскільки це можливо, так, щоб нова публічна інформація могла створюватися та використовуватися без державного втручання, наразі “пересічний громадянин” має розглядатися як “дистриб’ютор публічної інформації” [8].

Ідея публічності відтепер реалізується через використання соціальних медіа в процесі обміну інформацією, які стали якісно новим явищем в системі горизонтальних інформаційних зв’язків та створили принципово нову ситуацію в соціальній сфері суспільства, створивши умови для організації віртуальних соціальних утворень, і їх зростаючий вплив на суспільне життя.

Відтак, 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”.

Разом з тим, необхідною є розробка програм освітньо-виховного впливу, спрямованого на формування здатностей забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, оприлюднення власної інформації та способів її захисту, критичного ставлення до інформації.

Для успішного входження нашої держави в міжнародні інформаційні обміни вона має зосередитись насамперед на таких напрямах у сфері правової діяльності: розробляти систему правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток і ефективне використання в національних інтересах; здійснювати необхідну адаптацію національного інформаційного законодавства до загальновизнаної міжнародної правової бази з метою активізації своєї участі у інформаційних обмінах; брати активну участь у міжнародній правотворчості, що має оперативно регламентувати нові явища в сфері інформатизації; сформувати правову базу для регламентації участі у міжнародній діяльності по забезпеченню дотримання міжнародного інформаційного законодавства, боротьби з кібертероризмом та ін. видами інформаційної злочинності [9].

***Висновки.***

В умовах зростаючої активізації глобальних процесів у сучасному світі, що поряд із позитивними аспектами своїх впливів на світову спільноту створили також небезпеки інформаційної агресії, кіберзлочинності, саме загальнонаціональна система інформаційної безпеки, скоординована в своїй діяльності державою, може стати запорукою нейтралізації інформаційних загроз і використання позитивних факторів розвитку інформатизації.

Важливою складовою загальної політики забезпечення інформаційної безпеки України є підвищення участі громадськості у процесах удосконалення зв’язку “суспільство – держава”. Подальше зміцнення інформаційної безпеки країни вбачається у спільних, злагоджених діях усіх державних інституцій, громадськості, медіа-спільноти.

В сучасних умовах необхідно вирішувати не лише такі важливі завдання, як формування власного інформаційного простору та його захисту від загроз, а й переходити від захисних стратегій до наступальних.

## Використана література

1. Стратегія національної безпеки України : Указ Президента України від 26.05.15 р. № 287/2015. − Режим доступу : //www.president.gov.ua

2. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні // Юридичний вісник. – 2014. – № 2(31). – С. 59-65.

3. Онищенко О.С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотекака України ім. В.І. Вернадського. – К., 2014.

4. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції [“Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі”], (Харків, 26 жовтня 2012 р.). – Х. : НДІ державного будівництва та місцевого самоврядування, 2012. – 214 с.

5. Панченко В.М. Співвідношення понять : інформаційна та кібернетична безпека // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2 (12). – С. 20-24.

6. Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.

7. Горовий В.М. Правові перспективи національного розвитку. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#sthash.AgJjKJa4.dpuf

8. Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. – Режим доступу : //www.niss.gov.ua /articles/1730

9. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації // Правова інформатика. – 2013. – № 4(40). – С. 79-88.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~