**УДК 321.6+321.7+323.2**

**І. Малик**
Національний університет "Львівська політехніка"

# НАРОДЖЕННЯ "ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ": ВІД ТЕОРІЇ ДО ПРАКТИКИ



**Розглядаються актуальні проблеми інформаційної безпеки України загалом та її складові – особистості зокрема. Проаналізована діяльність держави у напрямку захисту інформаційно-психологічної безпеки особистості. Досліджено шлях прийняття 8 липня 2009 р. "Доктрини інформаційної безпеки України" та статті документа. Розглянуто проблему відновлення контролюючих функцій держави в інформаційній сфері, з огляду на забезпечення інформаційної безпеки України.**

***Ключові слова***: інформаційне суспільство, пропаганда, "Доктрина інформаційної безпеки України", інформаційна безпека особистості (суспільства, держави).

**Malyk Iryna**

# THE BIRTH OF "DOCTRINE OF INFORMATION SECURITY OF UKRAINE": FROM THEORY TO PRACTICE

**The article is dedicated to urgent problems of information security of Ukraine in general and its component – individuality – in particular. The State activity in reference to protection of information and psychological security of individuality is analyzed. The way of adoption on the 8th of July 2009 of "Doctrine of Information Security of Ukraine" is studied and articles of the document are analyzed. The issue of resumption of State controlling functions in the information field taking into consideration ensuring of information security of Ukraine is reviewed.**

***Keywords*:** Information society, propaganda, Doctrine of Information Security of Ukraine, information security of individuality (society, state).

**Актуальність дослідження**. На сучасному етапі розвитку глобального інформаційного суспільства, де кордони держав, з огляду на інформаційні потоки, робляться дещо умовними, а власні інформаційні потоки – всеохопними та безперервними, йдеться про одне з основних завдань державного утворення сучасності: підтримку та збереження балансу між дотриманням задекларованих демократичних принципів та збереженням власного інформаційного суверенітету.

**Мета роботи** – аналіз стану інформаційної безпеки України на сучасному етапі та дослідження діяльності української держави у цьому напрямку. Для цього необхідно виконати такі дослідницькі завдання: проаналізувати стан інформаційної безпеки особистості в Україні; вивчити та дослідити ймовірні моделі політики демократичного суспільства, необхідні для збереження інформаційної безпеки держави; проаналізувати діяльність держави щодо захисту особи від інформаційних впливів різного рівня; прослідкувати процес прийняття "Доктрини інформаційної безпеки України".

Новизною цього дослідження є аналіз діяльності держави загалом та України зокрема в забезпеченні інформаційної безпеки особистості, суспільства, держави. Зроблено спробу окреслити заходи, необхідні для гарантування інформаційної безпеки держави. Для цього проведено аналіз "Доктрини інформаційної безпеки України" – від історії її створення до спроб реалізації та втілення у життя.

Дослідженням закономірностей функціонування інформаційної сфери та інформаційної безпеки держави на сучасному етапі займаються такі українські вчені-дослідники, як В. А. Ліпкан, Ю. Є. Максименко, В. Я. Василюк, В. М. Желіховський, С. О. Климчук, В. О. Карпенко, О. В. Литвиненко.

***Виклад основного матеріалу***. Інформаційна сфера суспільства була та залишається особливо чутливою до зовнішніх впливів в умовах розвитку та становлення демократичних інститутів. Адже залишаються не виробленими необхідні стійкі фільтри: механізми відбору потрібного продукту споживання чи захисту від нього. Майже неминуче за таких умов будь-яка країна може стати об'єктом спланованого інформаційного впливу. І у разі, коли немає формули захисту від інформаційної небезпеки чи правил існування в умовах інформаційної безпеки, постає загроза не лише інформаційному суверенітету, але й державному. Адже інформаційна безпека особистості (суспільства, держави) – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо [1, с. 41].

Українському досліднику спеціальних інформаційних операцій О. В. Литвиненку вдалось прослідкувати цікаву закономірність: надійний захист від інформаційних впливів та спеціальних інформаційних операцій може забезпечити лише відкрита ідейна система, тобто така, що не концентрується на собі, а прагне до найбільшого поширення, доки вона не втрачає привабливості для оточуючих. Альтернативою цьому може бути тільки застосування найжорсткіших, майже тоталітарних методів контролю, які до того ж дають доволі короткотривалий або обмежений ефект [6]. Найяскравішим прикладом цього є існування в СРСР системи, яка здійснювала тотальний контроль над усіма сферами суспільного життя. Проте така система з часом вичерпує себе, адже неможливо повсякчасно, протягом довгого періоду, безперервно, без огляду на загальносвітові процеси, залишатись ізольованими та розвиватись всупереч суспільним законам. Тотальний контроль та цензура не лише захищають від "ворожих" інформаційних впливів, але й виступають неминучим бар'єром обміну інформацією. Це, своєю чергою, гальмує розвиток суспільних процесів та перешкоджає суспільному прогресу (яскравий приклад – "безкоштовна" радянська медицина, яка, з огляду на закритість суспільства, неможливість обміну інформацією та фаховим досвідом, залишалась на дуже низькому технічному рівні і працювала лише за рахунок "людського фактора").

Жорсткі методи захисту від інформаційно-психологічного впливу у певному сенсі є найпростішими та найзрозумілішими. Прийнято вирізняти дві основних форми державного контролю (цензури): *прямий та опосередкований*. Прямий контроль (цензура), своєю чергою, поділяється на *попередній і наступний* контроль [6].

*Попередній* контроль був здебільшого поширений до початку нашого століття в усіх країнах світу, але зараз здійснюється лише у диктатурах та під час надзвичайного чи воєнного стану. Його суть полягає у тому, що відповідний урядовець (цензор) переглядає пресу до її виходу у світ та дозволяє чи не дозволяє публікацію. Прикладом такого контролю може бути існування в Україні на рубежі тисячоліть (період правління Л. Кучми) так званих "темників" на телебаченні та у пресі, коли обирались певні теми-табу для висвітлення та публічного обговорення в суспільстві. *Прямий наступний* контроль з використанням засобів судового переслідування (і не тільки) застосовується у багатьох сучасних державах. Журналіст в авторитарному суспільстві перетворюється на джерело небезпеки та потребує постійного контролю з боку правлячої влади (еліти, ідеології тощо), звісно ж, в інтересах забезпечення існуючого статус-кво, тобто авторитаризму. Журналіст у тоталітарному суспільстві менш небезпечний – адже він чітко усвідомлює, що його існування та існування його родини залежить від його лояльності до правлячого режиму. *Опосередкований* контроль передбачає

застосування економічних важелів щодо ЗМІ з метою коригування їхньої політичної лінії. Зрозуміло, що ця форма контролю найпоширеніша у сучасних демократичних суспільствах. Цей вид контролю здійснює цілеспрямований економічний вплив на ЗМІ.

Оскільки на державному рівні одним з методів захисту від інформаційних впливів та операцій є контрпропаганда, то доцільно розглянути етимологію цього терміна.

Пропаганда (лат. *propaganda* – "те, що підлягає розповсюдженню") – розповсюдження різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою їх впровадження в масову свідомість суспільства та активізацію використання цих ідей у масовій практичній діяльності населення. Одночасно до пропаганди належать повідомлення, які розповсюджуються для здійснення вигідного впливу на суспільну думку, провокування запрограмованих емоцій та зміни ставлення чи поводження певної групи людей в напрямку, прямо чи опосередковано вигідному організаторам [13, с. 33].

Пропаганда – це систематичне, цілеспрямоване розповсюдження за допомогою різних засобів зв'язку та передачі інформації певних ідей з метою здійснення впливу на думки, переконання, почуття, відношення та поведінку на об'єктів пропаганди з метою отримання переваг, прямих чи не прямих [9; 10].

Контрпропаганда – це боротьба з ідеологічною пропагандою противника; одна з функцій пропаганди та форм пропагандистської діяльності. Отже, у цьому контексті співвідношення між пропагандою та контрпропагандою складається за формулою "дія-протидія". Найкраща контр-пропаганда – це наступальна пропаганда. Тобто сила контрпропаганди – у послідовному викритті неправоти противника. Зрозуміло, що викриття неправоти не зводиться лише до реагування на його напади. Найефективніша контрпропаганда – це випереджальна, наступальна пропаганда, яка працює на випередження та спроможна вгадувати напрямки атак противника [12; 9, с. 3–21].

Зрозуміло, що існують і специфічні контрпропагандистські прийоми. Одну з можливих класифікацій детально проаналізував у своїй праці О. В. Литвиненко [6]:

1. Парасолька. Суть цього прийому полягає у створенні захисної парасольки над аудиторією, наприклад, глушіння радіоголосів. За часів існування СРСР періоду "холодної війни" такі прийоми застосовувались доволі широко – "глушились" "Голос Америки" та "Радіо "Свобода".

2. Лійка. Пропагандистське повідомлення фактично зникає у масі інших, спеціально згенерованих у так званому інформаційному шумі.

3. Колесо. Нейтралізація повідомлення у свідомості за допомогою внесення пріоритетніших, важливіших повідомлень.

4. Заміна. Зміщення акценту з найнебезпечнішого аспекта повідомлення на інші.

Отже, завдання держави полягає у забезпеченні захисту інформаційного простору та контролю над ним. Цього можна досягти, лише створивши прозорі правила гри на інформаційному полі, що, своєю чергою, забезпечить реалізацію таких необхідних стратегій:

- створення потужних інформаційних потоків, що підтримуватимуть національну систему символів, установок, переконань та стереотипів, а також забезпечуватимуть їхню експансію у навколишній світ (за принципом "дія-протидія");
- введення необхідних обмежень доступу до інформації, контроль проходження інформаційних потоків та джерел (дотримуючись при цьому принципів демократичності, що підтверджено у Конституції України (Гл. 1, ст. 3–4, Гл. 5, ст. 32–35) [5].

Створити відповідні правила гри на інформаційному полі покликана була "Доктрина інформаційної безпеки України", яка з'явилась на світ лише у 2009 р. (затверджена Указом Президента України від 8 липня 2009 року; для порівняння: схожий документ під назвою "Доктрина информационной безопасности Российской Федерации" був підписаний Президентом В. Путіним у 2000 р.). Появі цього документа передувала ціла низка подій, які, за детального аналітичного фахового розгляду, давали підстави стверджувати: в українському інформаційному полі та поза його межами проводяться сплановані інформаційні операції з метою дискредитації Української держави

загалом та процесів становлення і розвитку демократичних інститутів зокрема. Свідченням цього є "Кольчужний скандал", "Касетний скандал", "Газові російсько-українські війни" 2006–2009 рр. тощо.

Розробка цього важливого документа була покладена на Раду Національної безпеки та оборони України Президентом України, який підписав відповідний Указ 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" та який був введений в дію Указом Президента України № 377 від 23 квітня 2008 року [14]. Як стверджувалось в офіційному друкованому органі Ради Національної безпеки та оборони України, у підготовці, обговоренні та узгодженні проекту було задіяно понад 30 органів державної влади, наукових установ, враховано понад 200 конкретних пропозицій, у тому числі від представників громадських організацій, експертного середовища [11]. Проект Доктрини розроблявся з урахуванням ролі і місця цього документа в системі нормативно-правового забезпечення національної безпеки в інформаційній сфері. Саме Доктрина повинна була розроблятись як документ такого рівня – концепції, стратегії, програми за певними напрямами, які мають загалом становити основу правового регулювання інформаційної сфери. Ціннісну характеристику проекту Доктрини становить визначення інформаційної безпеки як невід'ємної складової кожної зі сфер забезпечення національної безпеки і водночас важливої самостійної сфери національної безпеки України. Прийняття Доктрини інформаційної безпеки України покликане надати нового стратегічного імпульсу діяльності органів державної влади, а також інститутів громадянського суспільства у забезпеченні інформаційної безпеки України, формуванні і реалізації державної інформаційної політики.

Тож у "Доктрині інформаційної безпеки України" виділено основні складові національних інтересів України в інформаційній сфері та сформульовано принципи забезпечення інформаційної безпеки:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції [2].

Доктрина передбачає три основні напрями забезпечення державою національного інформаційного суверенітету:

1) законодавче визначення стратегічних шляхів розвитку та захисту національних ринків інформаційних та телекомунікаційних послуг на основі єдиної державної політики;

2) формування норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі;

3) визначення та захист національних інтересів в світовому інформаційному просторі та міжнародних інформаційних відносинах.

Важливими сьогодні є чітко сформульовані життєво важливі інтереси *держави* в інформаційній сфері:

- недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;
- ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері;
- побудова та розвиток інформаційного суспільства;
- забезпечення економічного та науково-технологічного розвитку України;
- формування позитивного іміджу України;
- інтеграція України у світовий інформаційний простір [2].

Величезним надбанням стало те, що Доктрина сформулювала реальні та потенційні загрози інформаційній безпеці України у таких сферах:

- зовнішньополітичній;
- сфері державної безпеки;
- воєнній сфері;
- внутрішньополітичній сфері;
- економічній сфері;
- соціальній та гуманітарній сферах;
- екологічній;
- науково-технічній.

Відповідно до сформульованих загроз у п. 4 Доктрини визначено напрями державної політики у сфері інформаційної безпеки України. Так, у зовнішньополітичній сфері держава зобов'язана займатися вдосконаленням інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном; забезпечити організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України; посилити інформаційно-просвітницьку діяльність серед населення щодо забезпечення національної безпеки України в разі повного її партнерства з державами–членами ЄС та НАТО; сприяти інтеграції в міжнародні інформаційно-телекомунікаційні системи та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету; гарантувати своєчасне виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізацію.

У сфері державної безпеки визначається доцільним залучення засобів масової інформації до забезпечення неухильного дотримання конституційних прав і свобод людини і громадянина, захисту конституційного устрою, вдосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства; розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп'ютерними системами і мережами.

Не може залишитись непоміченим і те, що важлива роль у забезпеченні задекларованих принципів відводиться засобам масової інформації як основному комунікатору і посереднику, який забезпечує обмін інформаційними потоками. Ще в середині XX ст. американський вчений та політолог Г. Лассуел виділив чотири основні функції ЗМІ:

- спостереження за світом (збір та розповсюдження інформації);
- "редагування" (відбір та коментування інформації);
- формування суспільної думки;
- розповсюдження культури [7, с. 91].

Адже, повертаючись до контролюючих функцій держави, необхідно усвідомити, що у випадку, якщо Україна не буде контролювати свої ЗМІ, то їх будуть контролювати інші держави. Поряд з цим українським журналістам доцільно виконувати вимоги Кодексу професійної етики українського журналіста, який був прийнятий на X з'їзді Національної спілки журналістів України у квітні 2002 року (в Російській Федерації Кодекс професійної етики російського журналіста був прийнятий значно раніше – Кодекс був затверджений Конгресом журналістів Росії 23 червня 1994 року) [4]. Зокрема, у п. 7 сказано, що "…журналіст у своїй професійній поведінці не має права ставити особисті інтереси понад усе. Замовчування чи поширення ним інформації шляхом одержання незаконних винагород або подання її як такої, що містить наклеп, упередженість, необґрунтовані звинувачення, – неприпустимі. Привласнення чужих думок і творів, матеріалів частково чи повністю (плагіат) суперечить професійній етиці журналіста, є підставою для осуду його з боку колег і оцінюється ними, як ганебний вчинок" [3].

**Висновки.** Отже, поява "Доктрини інформаційної безпеки України" встановила чіткі правила гри щодо забезпечення інформаційної безпеки держави. Доктрина чітко визначила та окреслила основні засади інформаційної безпеки України, встановила місце інформаційної безпеки в системі забезпечення національної безпеки України, виокремила реальні та потенційні загрози інформаційній безпеці України, сформувала напрями державної політики у сфері інформаційної безпеки держави. Появу Доктрини, з огляду на реалії сьогодення та повсякчасну безперервну боротьбу на різних рівнях в інформаційному просторі, неможливо переоцінити. Цей документ окреслює поле діяльності відповідних органів влади в справі збереження інформаційного суверенітету держави. Напрямок подальших наукових досліджень може стосуватися особливостей застосування та впровадження "Доктрини інформаційної безпеки" в українські реалії та її аналіз, з огляду на політичні реалії сьогодення.

*ЛІТЕРАТУРА:*

*1. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: "МК-Прес", 2005. – 431 с. 2. Доктрина "Інформаційної безпеки України" [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство. – Режим доступу до ресурсу: http://zakon. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009&p= 1267772861313087. 3. Кодекс Професійної етики українського журналіста (прийнятий на X з'їзді Національної спілки журналістів України (квітень 2002 року)) [Електронний ресурс] // Офіційний сайт компанії "Центра-Инвест": Мой проводник в мире прессы. – Режим доступу до ресурсу: http://centra.net.ua/old/codensju.htm. 4. Кодекс профессиональной этики российского журналиста (Кодекс одобрен Конгрессом журналистов России 23 июня 1994 года, Москва) [Електронний ресурс] // Право и СМИ (Право и средства массовой информации). – Режим доступу до ресурсу: http://www.medialaw. ru/selfreg/ 13/texts/276.htm. 5. Конституція України від 28.06.96. [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство. – Режим доступу до ресурсу: http:// zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=888-09. 6. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії [Електронний ресурс] / Литвиненко О. В. // Національний інститут стратегічних досліджень: Книги. – Режим доступу до ресурсу: http://www. niss.gov.ua/book/Litv/010_2.htm. 7. Панарин И. Н. Информационная война и выборы / И. Н. Панарин – М.: ОАО "Издательский Дом "Городец"", 2003. – 320 с. 8. Паречина С. Г. Методика подготовки и проведения публичных выступлений / С. Г. Паречина, А. Г. Караткевич. – Минск: ИСПИ, 2002. – 211 с. 9. Полевой устав Армии США FM 33-1. Психологические операции [Електронний ресурс] // "ПСИ-ФАКТОР". Центр практической психологи: Библиотека. – Режим доступу до ресурсу: http://psyfactor.org/lib/fm-33-1.htm. 10. Полевой устав армии США FM 33-1. Психологические операции. – М.: ГШ ВС СССР. – 1988. – 245 с.11. Проект Доктрини "Інформаційної безпеки України" [Електронний ресурс] // Рада Національної безпеки і оборони України: Новини. – Режим доступу до ресурсу: http://www.rainbow.gov.ua/news/930.html. 12. Роль и место контрпропаганды в агитационной работе: Доклад [Електронний ресурс] // ПТК легкой промышленности (Идеология): Учебные материалы. – Режим доступу до ресурсу: http://ptklp.minsk.edu.by/sm.aspx?uid=34100. 13. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і СІО: Навч. посіб. / В. М. Петрик [та ін.]. – К.: Росава, 2006. – С. 33. 14. Указ Президента України № 377/2008 "Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" [Електронний ресурс] // Офіційне Інтернет-представництво Президента України: Офіційні документи. – Режим доступу до ресурсу: http://www.president.gov.ua/documents/7773.html*