

ПОЛІТИКО-ПРАВОВІ АСПЕКТИ ДОСЛІДЖЕННЯ ФЕНОМЕНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Грицай Н.А.

студентка ФСП 6 курсу

НТУУ «КПІ»

В данной статье характеризуется явление информационной войны как угрозы национальным интересам и доказывается необходимость усовершенствования правового базиса в сфере информационной безопасности Украины как участника международных информационных отношений.

In this article the phenomenon of informative war is described as a threat for national interests and there is a necessity of improvement of legal base in the field of informative safety of Ukraine as participant of international informative relations.

В даній статті характеризується явище інформаційної війни як загрози національним інтересам та обґрунтовується необхідність удосконалення правового базису в сфері інформаційної безпеки України як учасника міжнародних інформаційних відносин.

Ключові слова: інформаційна війна, інформаційна безпека, правове забезпечення.

Актуальність дослідження.

Сучасний стан розвитку та використання інформаційно-комунікаційних технологій в контексті глобальних соціальних перетворень дозволяють називати сучасне суспільство розвинутих країн світу інформаційним. У такому суспільстві недопустима політично-правова некерованість суспільних відносин, що виникають з приводу обміну інформацією.

Україні як учаснику світового інформаційного простору необхідно приділяти більшу увагу збереженню національної, інтелектуальної, культурної та мовної самобутності. Це потребує розробки національної концепції та стратегії у сфері інформаційної безпеки шляхом визначення потреб і можливостей щодо масового використання інформаційних технологій в українському суспільстві. Досі відсутня цілісна система поглядів на захист інформаційного суверенітету держави, що відповідним чином позначається на рівні реалізації конституційних прав і свобод громадян, суспільства і держави в інформаційній сфері.

За таких обставин питання забезпечення інформаційної безпеки не може ігноруватися науковцями, дослідниками та державними службовцями в області національної безпеки. До аналізу політично-правового змісту феномену інформаційної безпеки, в першу чергу, спонукає поточний стан суспільно-політичного життя держави.

Метою даної статті є політико-правова рефлексія сутнісних характеристик інформаційної безпеки як реальної умови збереження національного суверенітету держави на прикладі України.

Для досягнення мети спробуємо вирішити наступні **завдання**:

- визначити сутність явища інформаційної війни як загрози національній безпеці держави;
- з'ясувати механізми, методи та цілі інформаційних війн;
- охарактеризувати особливості інформаційної безпеки України
- зробити короткий огляд українського законодавства у сфері інформаційних відносин.

• **Аналіз публікацій.** В наукових публікаціях останніх років як вітчизняних, так і закордонних вчених все частіше приділяється увага дослідженню таких феноменів, як "інформаційна війна", "інформаційне протиборство" та "інформаційна безпека". Серед найвідоміших вітчизняних дослідників, які зробили вагомий внесок у дослідження цих феноменів, можна виділити наступних. Л. Леонтєва в своїх працях аналізує стратегії ведення інформаційно-психологічної боротьби і проблеми інформаційно-психологічної безпеки, які при цьому виникають. А. Андрушко, М. Ожиган досліджують засоби ведення та наслідки інформаційних війн. В. Петренко та О. Юдін в своїх наукових статтях займаються проблематикою інформаційної безпеки, зокрема В. Петренко аналізує сутнісні аспекти інформаційної безпеки у процесі політичної комунікації в контексті мовного політичного маніпулювання. Безпосередньо вплив негативної інформації на широку аудиторію, маніпулювання суспільною свідомістю за допомогою ЗМІ в своїх працях досліджували А. Дутов, С. Кара-Мурза, Н. Куликова, Г. Маклаков, С. Муратов, Г. Почепцов, М. Солнцев, Л. Федотова.

Проблема інформаційної безпеки також розглядається в роботах І. Арістової, В. Бондаренко, В. Литвиненко, М. Карчевського, Б. Кормича, В. Остроухова, А. Стрельцова. Чільне місце у сфері дослідження інформаційної безпеки належить російським вченим С. Гриняєву та А. Левакову, які особливо активно досліджують інформаційні ресурси та можливості Сполучених Штатів Америки.

Однак, політико-правові засади забезпечення інформаційної безпеки України поки що не стали цілісним об'єктом дослідження науковців. У вищезгаданих роботах порушуються важливі, але лише окремі аспекти цього явища. З огляду на те, що українське законодавство є недосконалим в сфері інформаційної безпеки, необхідний комплексний, системний розгляд вищезазначеної проблеми.

Поряд з очевидними благами розвиток інформаційно-комунікаційного простору (ІКП) привносить і зовсім нові проблеми, серед яких: загострена цифрова нерівність країн і регіонів, проблема правового регулювання мережі Інтернет, електронної комерції й оподатковування в цій сфері, питання інтелектуальної власності, проблема забезпечення безпеки й конфіденційності інформації, можливість психологічного впливу на індивідуальну й суспільну свідомість з метою нав'язування свого бачення характеристик супротивника, його образу, використовуючи сучасні інформаційно-комунікаційні технології

Інформаційний чинник, який завжди впливав на рівень суспільного розвитку, зараз став виконувати головну роль при формуванні міждержавних відносин. Інформаційна сфера в сучасних умовах перетворилась на арену боротьби за світове лідерство та інформаційні впливи на відповідні країни і регіони. Нині інформація – це соціальна зброя, що використовується під час так названих інформаційних війн.

Оскільки поняття інформаційної війни є багатограним, то виникає проблема дати йому повне та вичерпне визначення. Серед відомих визначень найбільш вдалим, на думку автора, є визначення, яке дає Ю. Ноевий у своїй статті «Поняття інформаційно-психологічної боротьби та систематизація пов'язаних понять». Інформаційна війна – це найбільш напружена форма інформаційної боротьби, в якій сторони намагаються завдати шкоди інформаційно-технічним й управлінським системам, вплинути чи встановити контроль над інформаційним простором один одного, вплинути на погляди і поведінку армії та населення з метою перемоги над

супротивником в інформаційній царині та захиститися від шкоди, що наноситиметься супротивником [13].

Метою інформаційної війни виступає тотальний контроль інформаційного простору супротивника, який використовується для ведення інформаційних атак та забезпечення інформаційного домінування.

Учасники інформаційної війни розглядають інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активна протидія в інформаційному просторі [5].

Аналіз сучасних поглядів дозволяє вважати, що інформаційна війна у цілому є комплексом взаємопов'язаних і узгоджених за цілями, місцем і часом заходів, орієнтованих на досягнення інформаційної переваги. Невід'ємним поняттям інформаційної війни є поняття інформаційної зброї.

Інформаційна зброя представляє собою засоби знищення, викривлення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження або заборону доступу до них законних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, всього високотехнологічного забезпечення життя суспільства і функціонування держави [6].

Дослідник інформаційної війни С. Гриняєв називає наступні переваги інформаційної зброї, серед яких: **універсальність** (не залежить від кліматичних чи географічних особливостей місцевості ведення військових дій); **прихованість** (можливість приховати свої наміри нападати на супротивника); **економічна ефективність** (невеликі затрати); **можливість застосування** для вирішення **широкого кола завдань** (можна застосовувати на будь-яких етапах війни, на різних суб'єктів); **масштабність застосування** (можливе здійснення впливу на стаціонарні і мобільні елементи системи наземного, морського, повітряного і космічного базування); **володіння ефектом "ланцюгової реакції"** (вплив на одиничний елемент системи може привести до виведення з ладу інших елементів, сегментів і системи цілком); **складність здійснення міжнародного контролю** за розробкою і застосуванням (може бути надійно прихована від розвідок інших держав, різних міжнародних організацій, їх контролюючих органів) [7, с. 114].

Таким чином, інформаційна зброя, має на багато більше функціональних переваг перед військовою зброєю, адже несе тяжкі наслідки без кровопролиття та людських жертв, викликає величезні збитки без великих затрат, провокує соціальну нестабільність окремих груп суспільства та держави загалом. Такі переваги перетворюють інформаційну війну на реальну загрозу національним інтересам та вимагають жорстких захисних дій з боку національної політики в інформаційній сфері. Проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними загострюються внаслідок політичного й економічного протистояння держав. Все це стає актуальним у зоні забезпечення національної безпеки України.

На думку автора, головними суб'єктами загрозових інформаційних впливів виступають ініціатори тієї чи іншої провокації, організатори інформаційної атаки та реалізатори інформаційних операцій. Ініціаторами може виступати група людей (політичне, економічне, релігійне чи будь-яке інше об'єднання), а досить часто одна чи декілька держав, організаторами є група спеціалістів як в технічній, так і в управлінській сфері. Оскільки ЗМІ володіють потужними можливостями впливу на свідомість та поведінку людей, це дає підстави вважати ЗМІ головними реалізаторами інформаційних провокацій.

Враховуючи привабливість ЗМІ як інструменту соціального управління під час проведення інформаційних війн, варто оцінити ефективність його використання. Одним з параметрів ефективності є рівень довіри населення до ЗМІ.

Дозволимо собі посилатися на результати соціологічного дослідження «Ріст довіри до парламенту: тенденція чи тимчасове явище?», виконаного TNS Ukraine у вересні 2010 року. За його результатами вітчизняним ЗМІ повністю або переважно довіряють 50,8% українців, російським ЗМІ - 41,4%, а західним ЗМІ - 33,6%.

Традиційно для українського суспільства, найбільше громадяни довіряють церкві - 68,2% респондентів засвідчили повну або ж перевагу довіри їй. Друге місце посіли вітчизняні ЗМІ - їм довіряють 50,8% громадян. Також значний рейтинг довіри мають збройні сили - 43,5%. Російським ЗМІ українці довіряють більше, ніж президенту України - 41,4% проти 41,3% [9].

При такому високому рівні довіри громадян до вітчизняних, і не тільки, ЗМІ, стає можливим маніпулювання суспільною

думкою українців за допомогою "блакитних" екранів, радіохвиль, сторінок "жовтих преси" та веб-сторінок в Інтернеті. Насаджування чужих цінностей, дезінформація народу, підміна понять, зміна ідеалів та пріоритетів в майбутньому призводить до сепаратистських настроїв, розділення суспільства на антагоністичні групи. Відсутність єдиної сформованої національної позиції, в свою чергу, ускладнює процес збереження національного суверенітету.

Відповідно до Закону України "Про основи національної безпеки України" до загроз національним інтересам і національній безпеці в інформаційній сфері відносять: обмеження свободи слова та доступу громадян до інформаційних ресурсів, поширення ЗМІ культу насильства, жорстокості та порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [11].

В наш час всі ці загрози є не тільки на папері, але й у реальному житті українського суспільства. Спроби формування і реалізації державної інформаційної політики знайшли відображення в законах України «Про основи національної безпеки України» [3], «Про концепцію національної програми інформатизації» [1], «Про національну програму інформатизації» [2], а також у Стратегії національної безпеки України, яка затверджена указом Президента [4]. Розглянемо принципові питання щодо удосконалення правового регулювання у сфері інформаційної політики.

У зв'язку з тим, що правотворчий процес в нашій країні нерідко здійснюється без узгодження з чинним законодавством та світовими стандартами, було б доцільним в подальшому забезпечувати всебічне юридичне обґрунтування, передусім визначальних системоутворюючих понять, таких як: інформаційний суверенітет та національний інформаційний простір; правовий режим інформації і принципи міжнародного інформаційного співробітництва, що регламентують поведінку суб'єктів інформаційних відносин України в процесі формування, поширення, використання і захисту інформаційних ресурсів при здійсненні міжнародного інформаційного обміну.

Правові норми, що регламентують діяльність, пов'язану з формуванням і забезпеченням реалізації державної інформаційної політики щодо управління і захисту інформаційних ресурсів, повинні чітко визначати повноваження, права й обов'язки кожного суб'єкта інформаційних правовідносин [12].

Реалізація інформаційного суверенітету може функціонувати в декількох напрямках. В першу чергу, необхідне законодавче визначення та державне забезпечення стратегічних напрямів розробки цілісної інформаційної політики та захисту національного інформаційного простору. Враховуючи те, що Україна замає місце в світовому інформаційному просторі, варто визначити норми, засади, межі діяльності зарубіжних та міжнародних суб'єктів інформаційних відносин. Глобальний характер інформаційних відносин викликає формування та захист інтересів України в даній сфері.

Майбутній закон, на думку автора, який охоплював би проблему повністю, мав би забезпечити вирішення ряду завдань. Серед них перше місце займає створення єдиної державної інформаційної політики, без чого неможливе ефективне обстоювання національних інтересів держави. Одним з актуальних завдань є організація захисту українського інформаційного простору від неконтрольованого використання його зарубіжними суб'єктами інформаційної діяльності. повернути український телерадіоефір у площину українських національних інтересів. В цьому необхідно орієнтуватися на правову практику країн Західної Європи [8].

Висновки і рекомендації. Оскільки на рівні правового регулювання інформаційної сфери українське законодавство має суттєві недоліки, то некерованості процесів, що протікають в інформаційному просторі, й надалі залишатиметься загрозою національним інтересам України. Перш за все, явище інформаційної війни є реальною небезпекою для національного суверенітету України. Загальнонаціональний рівень важливості проблеми інформаційної безпеки країни, її комплексний характер вимагають розробки і реалізації відповідної національної довгострокової програми.

Заходи щодо забезпечення інформаційної безпеки України повинні включати: визначення складу, послідовності і алгоритму розробки законодавчих і нормативно-правових актів з питань інформаційної безпеки, а також механізмів їх введення в дію (правове забезпечення); розробку державної цільової науково-технічної програми забезпечення

інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення); розробку і створення організаційної структури системи інформаційної безпеки України (управлінське забезпечення); створення вітчизняної системи сертифікації технічних і програмних засобів інформатизації на відповідність вимогам інформаційної безпеки (організаційне забезпечення); забезпечення реальних потреб системи інформаційної безпеки в кадрах, матеріально-технічних і фінансових коштах (ресурсне забезпечення).

Пріоритетом в розробці стратегій інформаційної безпеки має стати створення законодавчої та нормативно-правової бази забезпечення безпеки, а саме розподілу і використання персональної інформації з метою створення умов для інформаційних стосунків між органами державної влади і суспільства, формування передумов досягнення соціального компромісу, створення умов соціального партнерства, реєстру інформаційних ресурсів, закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки. Неодноразово на розгляд Верховної Ради України потрапляли найрізноманітніші проекти законів про інформаційну безпеку, але жоден з них не був прийнятий в силу того, що вони являють собою довідники визначень, а не чіткий алгоритм дій або стратегію в області створення інформаційної безпеки. Інформаційна безпека в сучасному світі, в якому основним товаром є інформація, є основою національної безпеки.

Правовим базисом державної інформаційної політики є сукупність норм права і правових механізмів їх реалізації. Забезпечення інформаційної безпеки в політико-правовому аспекті має базуватися на наступних принципах. Додержання суверенного права України на формування, розвиток і використання національного інформаційного простору, правовий контроль розвитку складових національного інформаційного простору; гарантування кожному суб'єкту інформаційних відносин України прав на інформацію й свободу інформаційної діяльності, закріплених конституційними правовими нормами, незалежно від політичного, соціального і економічного статусу; обмеження доступу закордонних та міжнародних суб'єктів інформаційних відносин до інформаційного простору України; створення загальнодержавної системи регулювання суспільних інформаційних відносин,

пов'язаних із захистом інформаційних ресурсів.

Тільки на рівні закону можна сформулювати загальнодержавну систему інформаційної безпеки, вирішити питання охорони і захисту інформаційного простору.

Отже, нагальною потребою сьогодення, поряд із заходами, спрямованими на проведення реформи інформаційного законодавства та кодифікації правових норм регулювання суспільних інформаційних відносин, є розробка нових законів та підзаконних нормативно-правових актів щодо удосконалення системи управління і захисту інформаційних ресурсів України.

Література:

1. Закон України «Про концепцію національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – ст. 182.
2. Закон України «Про національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – ст. 181.
3. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – ст. 351.
4. Указ Президента України «Про Стратегію національної безпеки України» від 12 лютого 2007 року № 105/200.
5. Бабенко Ю. Інформаційна війна - зброя масового знищення. [Електронний ресурс]. — Режим доступу: <http://world.pravda.com.ua/rus/articles/2006/04/20/4399050/>
6. Балла І.В. Чи готова Україна до інформаційної війни. [Електронний ресурс]. — Режим доступу: http://mobilnyzakon.com.ua/index.php?option=com_docman&task=cat_view&gid=10&Itemid=2&lang=ru
7. Гриняев С.Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Мн.: Харвест, 2004. – 448 с.
8. Карпенко В.О. Інформаційна політика та безпека. [Електронний ресурс]. — Режим доступу: <http://ukrlife.org/main/karp/bezpeka.htm>
9. Лабораторія законодавчих ініціатив. Результати соціологічного дослідження на тему: «Ріст довіри до парламенту: тенденція чи тимчасове явище?». [Електронний ресурс]. — Режим доступу: <http://www.parliament.org.ua/>
10. Ліпкан В.А. Національна безпека України. [Електронний ресурс]. — Режим доступу: http://pidruchniki.com.ua/00000000/politologiya/natsionalna_bezpeka_ukrayini_-_lipkan_va
11. Манойло А.В., Фролов Д.Б., Інформаційно-психологічні операції як організаційна форма реалізації концепції інформаційно-психологічної війни, С.Пб.: Проблеми інформаційної безпеки. Комп'ютерні системи, 2003 р. № 2, с. 7-14.
12. Соснін О.В., Шиманський Л.Є. Про правові основи удосконалення системи державного управління інформаційними ресурсами. [Електронний ресурс]. — Режим доступу: http://old.niss.gov.ua/book/Pr17_04.htm
13. Ноєвий Ю.М. Поняття інформаційно-психологічної боротьби та систематизація пов'язаних понять. [Електронний ресурс]. — Режим доступу: http://www.nbu.gov.ua/portal/Soc_Gum/Gileya/2010_32/Gileya32/P3_doc.pdf