Інформаційна безпека як основа національної безпеки

І. Р.Боднар[i]

Державна інформаційна політика є важливою складовою зовнішньої і внутрішньої політики країни та охоплює всі сфери життєдіяльності суспільства. Бурхливий розвиток інформаційної сфери супроводжується появою принципово нових загроз інтересам особистості, суспільства, держави та її національній безпеці. У статті розглянуто складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни і визначені основні напрямки діяльності органів державної влади у цій сфері. Проаналізовані внутрішні та зовнішні інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки країни. Інформаційна безпека розглядається як складова національної безпеки країни, а також як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень. Запропоновані підходи щодо забезпечення процесу безперервності функціонування системи інформаційної безпеки держави з метою моніторингу нових загроз, визначення ризиків та рівнів їх інтенсивності.

Ключові слова: держава, політика, безпека, загрози,ресурси.

Абревіатури:
БІ – безпека інформації
НБ – національна безпека
ІР – інформаційний ресурс

УДК 65.012.8:007+32(477) *JEL коди:* D80, L98

Вступ. Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством. В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства та держави вимагають найшвидшого законодавчого регулювання.

Постановка проблеми. Проведення вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої

[i] *Боднар Ірина Романівна,* кандидат економічних наук, доцент, доцент кафедри міжнародних економічних відносин Львівської комерційної академії.

національної інформаційної стратегії в значній мірі сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній,соціальній, економічній та інших сферах державної діяльності.

Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені як Арістова І. [1], Почепцов Г. [2] та ін. Ряд публіцистів Супрун В. [3], Ярочкін В. [4] розробили основні принципи забезпечення інформаційної безпеки. В той же час, окремого дослідження вимагають структурно-функціональні аспекти процесу гарантування інформаційної безпеки.

Метою дослідження є виявлення та аналіз основних напрямів державної інформаційної політики з метою захисту національного інформаційного простору та гарантування інформаційної безпеки.

Результати дослідження. У ст. 17. Конституції України зазначено: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу" [5]. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України [6], захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз.

Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам [7] та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо.

Деякі засоби, які зараз прийнято відносити до інформаційної зброї, такі, наприклад, як спеціальні психологічні операції, існують та активно застосовуються досить давно, інші, зокрема, специфічні комп'ютерні засоби боротьби, з'явилися лише кілька років тому. Але всі вони мають дещо спільне – вони засновані на ідеї опосередкованого впливу на матеріальний світ.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні. Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати як поняття рівня інформаційної озброєності держави, так і механізм еволюції ресурсного потенціалу конкретної держави та вплив зовнішнього оточення. В даному випадку за основу аналізу вибраний інформаційний стан України.

Як базову розглянемо модель вирішення інформаційного конфлікту двох країн, яка складена на основі моделі Річардсона-Каспарова [8]. В основу моделі покладені наступні гіпотези:

- у процесі інформаційних атак кожна з двох країн прагне забезпечити зростання ефективності своєї інформаційної зброї пропорційно рівню інформаційності суперника;
- економічний потенціал кожної з країн надає/обмежує вплив на темп зростання інформаційних потужностей країни;
- держави ініціюють збільшення рівня інформаційних потужностей, керуючись власними прагненнями.

Введемо позначення N_1 (t), N_2 (t) рівнів інформаційних потужностей кожної з сторін конфлікту, де t – час. Тоді перераховані вище умови дії моделі можуть бути формалізовані у вигляді системи двох звичайних диференціальних рівнянь:

$$\dot{N}_1 = M_1(L_1 - N_1)[1 - \exp(-p_1(k_1N_2 - a_1N_1 + g_1))];$$
$$\dot{N}_2 = M_2(L_2 - N_2)[1 - \exp(-p_2(k_2N_1 - a_2N_2 + g_2))], \quad (1)$$

де M_1, $M_2, L_1, L_2, p_1, p_2, a_1, a_2, k_1$, k_2 – є позитивними коефіцієнтами, що не залежать від часу.

Параметри моделі (1) за аналогією Т. Сааті [4] визначені наступним чином:

k_1, k_2 – коефіцієнти реакції на інформаційні атаки;

a_1, a_2 – показники витрат на генерацію інформаційної зброї;

$g_1 g_2$ – коефіцієнти претензії (агресивності), якщо вони позитивні, або коефіцієнти доброї волі, якщо вони негативні;

M_1, M_2 – вартість наявного інформаційного забезпечення;

L_1, L_2 – граничні значення рівнів інформаційних потужностей;

p_1, p_2 – коефіцієнти ступеня важливості інформаційних витрат.

Модель (1) допускає існування чотирьох особливих розв'язків, що визначають координати положень рівноваги:

$$\text{а) } N_1^p = N_1^*, N_2^p = N_2^* \qquad \text{б) } N_1^p = N_1^*, N_2^p = L_2$$
$$\text{в) } N_1^p = L_1, N_2^p = N_2^* \qquad \text{г) } N_1^p = N_2^*, N_2^p = L_2 \quad (2)$$

деN_1^*, N_2^* – є рішення системи лінійних алгебраїчних рівнянь.

Нехай функції $u_1 = r_1^0(x_1 - x_2)$ і $u_2 = r_2^0(x_2 - x_1)$ характеризують політику кожної країни в сфері інформаційного протистояння, де змінних$x_1 = N_1 - N_1^*$, $x_2 = N_2 - N_2^*$мають значення відхилень від рівноважних рівнів інформаційної потужності. Тут r_1^0,r_2^0 – стаціонарні параметри управління. З врахуванням вигляду функціїu_1, u_2система (1) набуває вигляду:

$$\dot{x}_1 = M_1(\delta_1 - x_1)[1 - \exp(p_1(a_1x_1 - k_1x_2))] + r_1^0(x_1 - x_2);$$
$$\dot{x}_2 = M_2(\delta_2 - x_2)[1 - \exp(p_2(a_2x_2 - k_2x_1))] + r_2^0(x_2 - x_1). \quad (3)$$

Можна зробити такі висновки: кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки. Для цього необхідно:

- розуміння інформаційних атак та протистояння ним.

- створення програмного забезпечення протистояння інформаційним атакам;
- аналіз показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного управління;
- забезпечення максимального захисту від зовнішніх впливів;
- аналіз стану і технічний аудит всіх засобів комунікації;
- консолідація діяльності органів державної влади та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах криз та конфліктів.

В Україні всі види інформаційних технологій, їхнього виробництва та засоби забезпечення цих технологій становлять спеціальну сферу діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації. Визначення завдань Національної програми інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел і порядку їх бюджетного фінансування покладається на Кабінет Міністрів України і щорічно затверджується Верховною Радою України.

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

- концептуальне засади політичної безпеки [9], її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;
- визначення об'єктів та цілей;
- визначення прийнятних з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками;
- визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози.

Україна також проводить активне співробітництво у галузі безпеки інформації в рамках програми НАТО "Безпека через науку". Ця програма використовує такі механізми підтримки у галузі інформаційної безпеки:

- гранти на налагодження та укріплення існуючих зв'язків;
- створення дослідницьких центрів;
- підтримка проектів досліджень.

Процес забезпечення безперервності гарантування інформаційної безпеки можна поділити на шість основних стадій (рис. 1).

Аналізуючи рис. 1 бачимо, що всі етапи взаємопов'язані в рамках державної системи забезпечення інформаційної безпеки. Державна політика забезпечення інформаційної безпеки країни визначає основні напрямки діяльності органів державної влади у цій сфері. Ці напрями обумовлені змістом національних інтересів держави, суспільства та особистості. По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством.

Рис. 1. Процес забезпечення безперервності функціонування системи інформаційної безпеки держави[авторська розробка]

Розглянемо основні структурні блоки рис. 1.

1. Розуміння безперервності функціонування системи забезпечення інформаційної безпеки держави. Ця фаза пов'язана з ідентифікацією критично важливих точок (об'єктів) захисту. Йдеться також про виокремлення основних внутрішніх та зовнішніх загроз, що можуть стати критичними для системи.
2. Стратегії забезпечення безперервності функціонування системи. В цьому випадку завдання зосереджуються на визначенні та доборі альтернативних рішень щодо відновлення системи з метою мінімізації загроз. Пошук рішень балансує між собівартістю систем захисту та їхньою ефективністю.
3. Розробка та впровадження. На цій фазі зусилля зосереджуються на структуруванні та документуванні Програми безперервності державного управління.
4. Розвиток культури інформаційної безпеки держави передбачає забезпечення процесу розробки державної інтегральної системи захисту інформації.

5. Виконання, підтримка та аудит процесу регулювання безперервного функціонування системи інформаційної безпеки держави за умов різноманітних криз та конфліктів.
6. Управління програмою інформаційної безпеки держави шляхом розподілу функцій, що передбачає відповідальність, страхування (гарантії) та керування у контексті реалізації загального плану безперервності функціонування системи забезпечення інформаційної безпеки держави.

Якщо наноситься шкода в результаті недосконалості інформаційних відносин, використанні неякісної інформації тощо, то це свідчить про зниження інформаційної безпеки [10]. Це дає змогу розглядати як невирішені проблеми гарантування інформаційної безпеки в Україні:

- недосконаліть інформаційної політики та політики інформаційної безпеки держави;
- недосконаліть нормативно-правової бази в сфері інформаційних відносин та інформаційної безпеки;
- недостатню розвиненість інформаційної інфраструктури держави;
- введення іноземними державами обмежень по відношенню до України щодо розповсюдження інформації та отримання нових інформаційних технологій;
- протиправна діяльність посадових осіб, різних формувань та груп у сфері інформаційних інтересів громадян та держави;
- недосконаліть державної системи забезпечення інформаційної безпеки;
- можливість виникнення непередбачених ситуацій у системах та процесах, що базуються на використані інформаційних технологій.

Висновки і перспективи подальших наукових розробок. Державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведеної вище схеми створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності.

Основні акценти державної інформаційної політики повинні базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

Література

1. *Арістова, І. В.* Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія [Текст] / І. В. Арістова. – Х. : Нац. ун-т внутр. справ, 2006. – 354 с.
2. *Почепцов, Г.* Інформаційна політика: навч. посібник [Текст] / Г. Г. Почепцов. – К.: Знання, 2006. – 663 с.
3. *Супрун, В. М.* Інформаційний суверенітет як один з елементів інформаційної безпеки держави:

теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009.
4. *Ярочкін, В.* Система безпеки фірми [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua.
5. *Закон України.* Про інформацію/ [Електронний ресурс].– Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.
6. *Боднар, І. Р.* Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія [Текст] / І. Р. Боднар. – Львів : Видавництво Львівської комерційної академії, 2013. – 320 с.
7. *Бондаренко, В.* Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. Бондаренко, О. Литвиненко.– Режим доступу : http://www.crime-research.iatp.org.ua/library/strateg.htm.
8. *Саати, Т. Л.* Математические модели конфликтных ситуаций. – М. : Сов. Радио, 1977. – 304 с.
9. *Державна* інформаційна політика [Електронний ресурс]. – Режим доступу : http://merega.org.ua/law/projects/derzh polityka.
10. *Боднар, І. Р.* Роль держави у формуванні інформаційної політики [Текст] / І. Р. Боднар // Вісник ЛКА. – 2011. – Випуск 34. (Серія економічна). – С. 291–296.

Отримано 11.11.2013 р.

Информационная безопасность как основа национальной безопасности

ИРИНА РОМАНОВНА БОДНАР*

**кандидат экономических наук, доцент, доцент кафедры международных экономических отношений Львовской коммерческой академии, ул. Туган-Барановского, 10, г. Львов, 79005, Украина, тел.: 038-032-2448626, e-mail: iryna.bod@gmail.com*

Государственная информационная политика является важной составляющей внешней и внутренней политики страны и охватывает все сферы жизнедеятельности общества. Бурное развитие информационной сферы сопровождается появлением принципиально новых угроз интересам личности, общества, государства и его национальной безопасности. В статье рассмотрены составляющие государственной информационной политики по обеспечению информационной безопасности и определены основные направления деятельности органов государственной власти в этой сфере. Проанализированы внутренние и внешние информационные угрозы национальной безопасности Украины и пути обеспечения информационной безопасности страны. Информационная безопасность рассматривается как составляющая национальной безопасности страны, а также как глобальная проблема защиты информации, информационного пространства, информационного суверенитета страны и информационного обеспечения принятия правительственных решений. Предложены подходы по обеспечению процесса непрерывности функционирования системы информационной безопасности государства с целью мониторинга новых угроз, определения рисков и уровней их интенсивности.

Ключевые слова: государство, политика, безопасность, угрозы, ресурсы.

Mechanism of Economic Regulation, 2014, No 1, 68–75
ISSN 1726-8699 (print)

Information Security as the Foundation of National Security

IRYNA R. BODNAR*

[*] *C. Sc. (Economics), Associate Professor, Department of International Economic Relations, Lviv Academy of Commerce, Tugan-Baranovsky Street, 10, Lviv, 79005, Ukraine, phone: 00-380-32-2448626, e-mail: iryna.bod@gmail.com*

Manuscript received 11 November 2013

National information policy is an important component of foreign and domestic policy of the country and covers all areas of society. The rapid development of the information field is accompanied by fundamentally new security interests of the individual, society, the state and its national security. The components of the state information policy on information security and the basic activities of public authorities in this field are reviewed in the article. The internal and external information challenges facing Ukraine and ways of ensuring information security are analysed. Information security is seen as a component of national security, as well as a global problem of information security, information space, information sovereignty and information support decision-making. The proposed approach to ensure continuity of operation of the process of information security to monitor new threats, the risks and levels of intensity.

Keywords: government, politics, security, threats, resources.

JEL Codes: D80, L98 Figures: *1*; Formulas: 3; References: *10*

Language of the article: Ukrainian

References

1. Aristova, I. V. (2006), *Activity of the Interior to implement the state information policy*, Kharkiv, Nats. un-tvnutr. sprav. (In Ukrainian)
2. Pocheptsov, H. (2006), *Information Policy*, Kyiv, Znannia. (In Ukrainian)
3. Suprun, V. M. (2009), Information sovereignty as part of information security: theoretical and legal aspects, http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009. (In Ukrainian)
4. Yarochkin, V. (2012), The security system company, http://www.nbuv.gov.ua. (In Ukrainian)
5. The Law of Ukraine (1992), "On information," http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12. (In Ukrainian)
6. Bodnar, I. R. (2013), *Modern Realities of the Information Society: Problems of Establishment and prospects for development*, Lviv, Vydavnytstvo Lvivskoi komertsiinoi akademii. (In Ukrainian)
7. Bondarenko, V. and Litvinenko O. (2011), Information security of the modern state: conceptual reflections, http://www.crime-research.ru/library/strateg.html. (In Ukrainian)
8. Saati, T. L. (1977), *Mathematical models of conflict situations*, Moscow, Sov. radio.(In Russian)
9. *National Information Policy*, http://merega.org.ua/law/projects/derzhpolityka. (In Ukrainian)
10. Bodnar, I. R. (2011), "The state's role in shaping the Information Policy," *Visnyk LKA* (Ekonomika), 34, 291–96. (In Ukrainian)