

І. Р. Боднар,
к. е. н., доцент кафедри міжнародних економічних відносин,
Львівська комерційна академія

ПРІОРИТЕТНІ НАПРЯМИ ДЕРЖАВИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто ключові поняття та основи державної інформаційної політики в сфері інформаційної безпеки. Аналізується діяльність держави в інформаційній сфері, визначені основні напрями держави в сфері інформаційної безпеки. Запропоновані концептуальні підходи гарантування інформаційної безпеки.

Considered the key concepts and fundamentals of state information policy in the field of information security. Analyze the activities of the state in the information sphere, defines the main directions of state in the field of information security. The proposed conceptual approaches to ensure information security.

Ключові слова: інформаційна безпека, інформаційні загрози, державна інформаційна політика, інформаційні ресурси, інформаційне суспільство, національна безпека.

Key words: information security, information threats, public information policy, information resources, information society, national security.

ВСТУП

Ризики, загрози й виклики детермінують масштаби людської діяльності. Відповідно за основу методології їхнього розуміння й обліку повинно бути покладене чітке усвідомлення якісного і кількісного аспектів ризиків, які виникають у кожному конкретному різновиді людської діяльності. Так, у процесі стратегічного планування США використовують два терміни: "загроза" (threat) і "виклик" (challenge). Вони позначають можливість якої-небудь країни, групи осіб або певного явища загрожувати ("загроза") або протидіяти ("виклик") досягненню цілей національної безпеки.

Інформаційна сфера та її державний захист виступають основою наукових досліджень вітчизняних та зарубіжних вчених. Вивченням ролі держави у формуванні інформаційного суспільства та забезпеченні інформаційної безпеки займаються такі вчені, як І.В. Арістова [1], К.І. Беляков [2], Г.Г. Почепцов [3], І. Рамоне [4], Д. Лук'яненко [4], Соснін О.[5] та ін.

Мета статті полягає у необхідності теоретичного обґрунтування діяльності органів державної влади, які здійснюють управління інформаційною сферою, реалізують інформаційну політику з метою захисту національного інформаційного простору та гарантування інформаційної безпеки.

НЕОБХІДНІ ВИЗНАЧЕННЯ

Інформаційна безпека у сучасному постіндустріальному світі, в якому основним товаром є інформація, яка впливає на прийняття державою тактичних та стратегічних рішень, є основою національної безпеки. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. Її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії значною мірою сприяло б досягненню успіху при вирішенні зав-

дань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, проведення вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. 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" [6]. Інформаційна безпека — це стан захищеності суспільства, держави, особистості, стан захищеності інформаційних ресурсів, які забезпечують прогресивний розвиток життєво важливих сфер для суспільства. 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 рівні інформаційної озброєності держави і механізм еволюції в залежності від ресурсного потенціалу конкретної держави та впливу зовнішнього оточення [7].

У даному випадку ми будемо брати за основу інформаційний стан України. Як базову розглянемо модель вирішення інформаційного конфлікту двох країн, яка складена на основі моделі Річардсона — Каспарова [8, с. 93]. В основу моделі покладені наступні гіпотези:

— у процесі інформаційного конфлікту кожна з двох держав прагне забезпечувати зростання ефективності своєї інформаційної зброї пропорційно рівню інформаційної потужності;

— економічний потенціал кожної з країн надає/обмежує вплив на темп зростання інформаційних потужностей;

— державні установи ініціюють збільшення рівня інформаційних потужностей, керуючись своїми прагненнями.

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

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

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 з термінологією Т. Сааті [8, с. 23] визначені наступним чином:

k_1, k_2 — коефіцієнти реакції або захисту від інформаційного впливу суперника;

a_1, a_2 — індикатори відносних 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 утримання наявного інформаційного озброєння;

L_1, L_2 — граничні значення рівнів інформаційних потужностей, що залежать від обсягів ресурсів кожної із сторін;

p_1, p_2 — коефіцієнти ступеня важливості інформаційних витрат.

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

$$\begin{aligned} \text{а) } N_1^* &= N_1^*, N_2^* = N_2^* & \text{б) } N_1^* &= N_1^*, N_2^* = L_2 \\ \text{в) } N_1^* &= L_1, N_2^* = N_2^* & \text{г) } N_1^* &= N_1^*, N_2^* = L_1 \end{aligned} \quad (2),$$

де N_1^*, N_2^* — 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 змінні $x_1 = N_1 - N_1^*$, $x_2 = N_2 - N_2^*$ мають значення відхилень від рівноважних рівнів інформаційної потужності. Тут r_1^0, r_2^0 — стаціонарні параметри управління. З врахуванням вигляду функції система (1) набуває вигляду:

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

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

— розуміння інформаційного протистояння як феномена, що має певну логіку розвитку;

— створення математичних моделей та на їх базі — сценаріїв ведення інформаційної війни;

— вироблення кількісних і якісних показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень у системах державного і військового управління;

— розроблення програмного продукту на базі національного науково-виробничого потенціалу для забезпечення максимального захисту від зовнішніх впливів на комп'ютерні комунікації;

— аналіз стану і технічний аудит всіх засобів інформаційної війни з урахуванням їх відповідності сучасним вимогам;

— консолідація діяльності органів державної влади, політичних партій та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу на соціум.

Заходи держави в сфері інформаційної безпеки.

В Україні інформація поділяється на два різновиди — таємну та конфіденційну. Відповідно до Закону України "Про інформацію", до таємної інформації відносять такі відомості, розголошення яких завдає шкоди особі, суспільству і державі вона включає до свого складу державну або іншу, визначену законом, таємницю. Перелік видів таємної інформації визначається державою і закріплюється законодавчо. Державна таємниця включає в себе відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені у встановленому законом порядку державною таємницею і підлягають охороні державою [6].

З метою нейтралізації загроз інформаційно-психологічного впливу на масову та індивідуальну свідомість, що можуть завдати збитків суспільному та індустріальному здоров'ю, а також зловживання свободою масової інформації доцільним і невідкладним є опрацювання єдиної державної політики у сфері забезпечення інформаційно-психологічної безпеки та відповідної нормативно-правової бази, спрямованих на вирішення наступних завдань:

— координацію діяльності органів державної влади і суспільно-громадських об'єднань, розмежування повноважень органів державної влади та місцевого самоврядування у відповідній сфері;

— встановлення розумних балансів "стримувань та противаг" між потребою у вільному обміні інформацією і припустимими обмеженнями щодо її поширення;

— збереження єдиного інформаційного і духовного простору України, традиційних підвалин суспільної моральності;

— розвиток правосвідомості та психологічної культури громадян у сфері психологічно-інформаційної безпеки;

— навчання населення методам самозахисту від негативних інформаційних впливів, основам безпечної поведінки в сучасному інформаційному середовищі;

— розвиток і підтримку вітчизняного виробництва засобів захисту від негативних інформаційно-психологічних впливів;

— організацію міжнародного співробітництва щодо забезпечення інформаційної безпеки;

— створення вітчизняної системи ліцензування, сертифікації, експертизи і контролю в сфері інформаційної безпеки;

— розробку і прийняття стандартів у сфері інформаційної безпеки;

— експертизу з метою виявлення негативних інформаційно-психологічних впливів та обов'язкового ліцензування діяльності і забезпечення інформаційної безпеки і сертифікацію відповідних засобів і методів.

Нижче пропонується структурна схема поетапного становлення та функціонування системи інформаційної безпеки Української держави (рис. 1).

Аналізуючи рис. 1, бачимо, що забезпечення безперервності та оперативної трансформації системи залежить від її спроможності реагувати на нові виклики й ризики, що передбачає виконання основних стадій на-



Рис. 1. Структурна схема поетапного становлення та функціонування системи інформаційної безпеки України

Складено за [7].

гляду за системою забезпечення інформаційної безпеки держави, а саме:

- безпосереднє впровадження механізмів забезпечення необхідного рівня безпеки;
- моніторинг системи та її реакції на інциденти (події) і впровадження політичної безпеки із використанням ефективних інструментів відстеження різноманітних "вторгнень";
- тестування системи безпеки через постійне вдосконалення аудиту;
- вдосконалення системи.

Забезпечення безперервності функціонування системи інформаційної безпеки держави є одним із основних завдань державної політики у сфері як національної безпеки загалом, так і забезпечення інформаційної безпеки держави зокрема. 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:

- стисле концептуальне пояснення зацікавленим суб'єктам політичної безпеки, 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 [9].

В Україні назріла об'єктивна потреба у такому 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. Найскладнішими тут є такі завдання:

- гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів;
- керування не лише власними інтересами, але й національними інтересами інших країн;

— врахування реалій сучасного світового інформаційного простору, який рухається до неподільності та формування глобального інформаційного суспільства.

ВИСНОВКИ

Критично важливою є необхідність практичної реалізації наведеної вище схеми створення ефективної системи інформаційної безпеки держави. З цією метою доцільне опрацювання "Доктрини національної інформаційної безпеки України" з чітким визначенням зон (сфер) відповідальності органів виконавчої влади щодо забезпечення кожного з етапів функціонування інформаційної безпеки держави згідно з наведеною схемою. Предметом постійної уваги в межах визначеного доктриною часового проміжку має стати перегляд списку "Загроз національній безпеці України в інформаційній сфері" як щодо нових загроз, так і усунення наявних із визначенням ступеня можливих наслідків та рівнів інтенсивності.

З огляду на те, що проблема забезпечення безперервності функціонування системи забезпечення інформаційної безпеки держави є ключовою, пріоритетним є також створення/відновлення основних напрямів захисту системи національної безпеки в інформаційній сфері. Пошук рішень має бути продиктований балансом собівартості подібної системи захисту та її ефективності. З метою практичної реалізації зазначеної стратегії слід створити інтегрований у вертикаль виконавчої влади спеціальний орган, який здійснював би її практичну реалізацію і на який, окрім функції впровадження, були покладені обов'язки запуску власне самого процесу розбудови інтегральної системи забезпечення інформаційної безпеки держави, контролю за її виконанням та формулювання нових стратегій з урахуванням кардинальних змін у геостратегічній ситуації України.

Література:

1. Арістова І.В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: монографія / І.В. Арістова. — Х.: Нац. ун-т внутр. справ, 2006. — 354 с.
2. Беляков К.І., Інформаційні технології як фактор терористичного акту [Електронний ресурс]. — Режим доступу: http://www.mndc.nai.au.kiev.ua/Gurnal/8text/g8_12.htm841/30.pdf.
3. Почепцов Г.Г. Інформаційна політика: навч. посібник / Г.Г. Почепцов — К.: Знання, 2006. — 663 с.
4. Рамоне І. Глобальні трансформації та стратегії розвитку: монографія / Рамоне І., Лук'яненко Д.— К., 2010. — 453 с.
5. Соснін О. Державне управління інформатизацією як виклик цивілізаційного зростання нації / Соснін О. / Зовнішні справи. — 2011. — № 9. — С. 38—41.
6. Закон України "Про інформацію" [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12>
7. Веб-сторінка інституту стратегічних досліджень [Електронний ресурс]. — Режим доступу: <http://www.niss.gov.ua>
8. Саати Т.А. Математические модели конфликтных ситуаций. — М.: Сов. Радио, 1977. — 304 с.
9. Державна інформаційна політика [Електронний ресурс]. — Режим доступу: <http://merega.org.ua/law/projects/derzhpolityka>.

Стаття надійшла до редакції 09.11.2011 р.