Марина БАБІНСЬКА

ПРОБЛЕМИ ШФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Житомирський державний університет імені Івана Франка, м. Житомир

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, проведення в життя 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".

Інформаційна безпека - це стан захищеності суспільства, держави, особистості, стан захищеності інформаційних ресурсів, які забезпечують прогресивний розвиток життєво важливих сфер суспільства.

Такі складові інформаційного середовища України, як інформаційні ресурси (у тому числі й інформаційні технології) та інформаційна інфраструктура (як матеріально-технічна основа створення, розповсюдження і використання інформаційних ресурсів), які входять до складу національного інформаційного потенціалу, сьогодні значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни. У наш час «інформаційний потенціал» стає одним з найважливіших чинників забезпечення національної безпеки наряду з «економічним потенціалом», «військовим потенціалом» тощо.

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.

В контексті використання інформації в якості зброї вона може характеризуватись такими показниками, як цілеспрямованість, вибірковість, роззосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на технічні засоби, системи і людей, можливість регулювання (дозування) „потужності" впливу, тощо, що визначає її як зброю масового ураження (5; 47).

В Україні зі становленням державності проблеми безпеки використання інформації набули особливої гостроти. Перехід від інформаційної ізоляції за часів СРСР до інформаційної відкритості сьогодення занурив українське суспільство у світові інформаційні процеси, які вимагають від України формування сучасних поглядів на роль і місце інформаційної складової в усіх сферах життєдіяльності. Одна з найважливіших проблем безпеки використання інформації - забезпечення управлінської діяльності органів державної влади. Переважна більшість рішень, що приймаються державними структурами, мають інформаційну основу.

Специфіка забезпечення національної інформаційної безпеки знайшла відображення в законах України „Про основи національної безпеки України», «Про концепцію національної програми інформатизації"", „Про національну програму інформатизації"", а також у Стратегії національної безпеки України, яка затверджена указом Президента .

У Законі „Про основи національної безпеки України" вперше дано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України (4; 351).

Ще в одному офіційному документі - „Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства в Україні" [4] ідеться, що стан розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України.

Основні шляхи і напрями реалізації концептуальних положень інформаційної безпеки держави мають бути зазначені в науково обгрунтованій доктрині інформаційної безпеки, якої на сьогодні в Україні немає. Вона, як правило, розробляється на визначений період. Доктрина

інформаційної безпеки держави є не тільки системою офіційно прийнятих поглядів щодо інформаційних та інших питань. Вона насамперед є керівництвом до дії. На основі доктринальних положень здійснюється широке коло політичних заходів і дій у зовнішній і внутрішній політиці держави. Доктрина інформаційної безпеки, будучи логічним продовженням Стратегії національної безпеки, розробляється законодавчими органами і політичним керівництвом держави. її основні вимоги деталізуються в законодавчому й іншому нормативно-правовому актах, висвітлені в стратегії розвитку держави у вигляді цільових державних програм і проектів.

Саме тому інформаційна безпека перетворюється на одну з ключових складових національної безпеки. Деякі дослідники вважають, що забезпечення інформаційної безпеки необхідно не тільки для того, щоб зберегти недоторканість національного інформаційного простору, але й наполягають на тому, що вірно сформульована національна інформаційна стратегія сприяла б більш успішному вирішенню задач у політичній, економічній, соціальній та інших сферах життя. Припускається також можливий вплив відповідної інформаційної політики на позитивний хід розв'язання як внутріполітичних так і зовнішніх конфліктів.

У Концепції Національної безпеки України визначаються основні можливі загрози національній безпеці держави в найбільш важливих сферах життєдіяльності, серед яких також наявні загрози, що стосуються інформаційної сфери:

невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері;

повільність входження України у світовий інформаційний простір, брак у міжнародного співтовариства об'єктивного уявлення про Україну;

інформаційна експансія з боку інших держав;

витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави;

запровадження цензури.

Слід визнати, що на сьогодні інформаційно-аналітичне середовище України досі перебуває у стані формування. У 1992 р. розпочав свою діяльність Національний інститут стратегічних досліджень, який за статутом є „урядовою інституцією для проведення досліджень, аналітичного прогнозування та стратегічного планування з метою забезпечення інформацією Ради національної безпеки і оборони та Президента України". З 1997 р. працює Національний інститут українсько-російських відносин. Продовжують наукову роботу відповідні інститути Національної академії наук України. Створюються незалежні інформаційно-аналітичні центри. Однак інформаційно-аналітичне середовище в нашій державі ще не повністю відповідає вимогам сучасності, воно вимагає певної корекції щодо незалежності науково-аналітичних інституцій від політичних внутрішніх та зовнішніх впливів, більш повного кадрового забезпечення.

Другою групою заходів по забезпеченню інформаційної безпеки є заходи, що здійснюють безпосередньо захист інформації. У даному випадку під захистом інформації мається на увазі система заходів, спрямованих на унеможливлювання несанкціонованого доступу до інформації, її зміни або знищення. Проблема захисту інформації розглядається у правовому полі (законодавчо-нормативне забезпечення) та у технічній сфері (безпосередньо технічне забезпечення безпеки інформаційних ресурсів). Деякі дослідники окремо виділяють страхування інформаційних ризиків, однак хотілось би зазначити, що цей вид діяльності не має великого розповсюдження на теренах України, хоча експерти і передрікають йому великі перспективи розвитку, що зростатимуть відповідно до збільшення обсягів інформації, якою оперує суспільство.

На відміну від відносно відсталої системи страхування інформаційних ризиків, робота по технічному забезпеченню безпеки інформації в Україні підтримується на належному рівні, і Майже всі державні і недержавні установи, що використовують у своїй роботі інформаційні ресурси, несанкціонований доступ до яких міг би спричинити збитки, включили в свою структуру відділи інформаційної безпеки. Розробка технічних засобів забезпечення безпеки І інформації здійснюється організаціями типу Українського Центру Інформаційної Безпеки.

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;

візити експертів та трансфер технологій;
створення дослідницьких центрів;
підтримка проектів досліджень.

В цілому співробітництво між НАТО та країнами-партнерами, одним з яких є і Україна, в рамках Ради євроатлантичного партнерства (РЄАП) та Програми „Партнерство заради миру" (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації. Для збільшення транспарентності військового планування й оборонних бюджетів і забезпечення демократичного контролю над збройними силами сторони можуть брати участь у взаємному обміні інформацією про кроки, що вони почали або починають. Перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи по безпеці інформації повинні бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити захист інформації відповідно до вимог сторони, яка її передає (1; 3).

Приєднання країни до програми ПЗМ передбачало ратифікацію „Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або програмі ПЗМ". Згідно цієї Угоди, сторони погоджуються консультуватися по політичних питаннях і питаннях безпеки, розширювати й інтенсифікувати політичне і військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах має на увазі обмін „таємною" інформацією і/або інформацією обмеженого доступу серед учасників. Відповідальним органом при захисті таємної інформації, якою обмінюються сторони при співробітництві в рамках РЄАП/ПЗМ, є Служба безпеки НАТО (NOS). Країна-партнер інформує Службу безпеки НАТО про те, який національний орган має повноваження в області безпеки інформації. Указом Президента України від 27 січня 2001 року "Про Державну програму співробітництва України з Організацією Північноатлантичного Договору (НАТО) на 2001-2004 роки" (ДПС-2004) на Державний комітет зв'язку та інформатизації України покладено відповідальність за реалізацію 5 розділу цієї програми, а саме "Співробітництво в галузі телекомунікаційних та інформаційних систем". Також, між НАТО та країною-партнером укладається окрема адміністративна угода по стандартах взаємного забезпечення безпеки інформації, якою обмінюються сторони і призначається офіцер зв'язку між Управлінням безпеки НАТО і національним уповноваженим органом по безпеці інформації. У травні 1998 р. на засіданні Комісії Україна - НАТО на рівні міністрів закордонних справ було погоджено призначення в Київ офіцера НАТО по зв'язках з метою сприяння повномасштабній участі України в ПЗМ і вдосконалення співпраці між військовими НАТО та України в цілому.

Вся інформація, якою обмінюються сторони в рамках РЄАП/ПРМ, є інформацією обмеженого доступу і тільки для урядового використання. Тому її повинні отримувати тільки організації й особи, які беруть участь у цих програмах і мають з нею справу за родом своєї діяльності. Установлення ступеня таємності документа або зниження ступеня таємності є прерогативою автора документа. На відміну від стандартів щодо захисту інформації, прийнятих в НАТО, де існує чотири рівні захисту, в мінімальних стандартах по обробці і захисту таємної інформації, якою обмінюються сторони в рамках програм РЄАП/ПЗМ, опущений рівень „абсолютно таємно", що спричинено тим, що кількість абсолютно таємної інформації в НАТО є дуже обмеженою, а додаткові вимоги по безпеці в зв'язку з цим рівнем таємності невиправдано ускладнили б правила обміну інформацією між країнами-партнерами і НАТО.

Певним досягненням стала ратифікація Законом України від 12 вересня 2002 р. „Угоди про безпеку між Урядом України та Організацією Північноатлантичного Договору", яка визначає основні вимоги щодо обміну та захисту таємною або конфіденційною інформацією між Україною та НАТО в рамках РЄАП та ПЗМ і може стати основою прийняття відповідних документів в процесі подальшого співробітництва чи повної інтеграції України в Альянс.

Законодавча база у галузі безпеки інформації також складається з Законів України „Про інформацію", „Про захист інформації в автоматизованих інформаційних системах", „Про державну таємницю" та ін. Діє також низка Указів Президента та Постанов Кабінету Міністрів України, які регулюють конкретні напрями діяльності в галузі захисту інформації.

Наступною групою заходів по забезпеченню інформаційної безпеки є заходи щодо захисту національного інформаційного простору від несанкціонованих втручань, а також контроль над системами формування масової свідомості. Національним інформаційним простором у даному контексті прийнято вважати сукупність інформаційних потоків, як національного, так і іноземного походження, які є доступними з території держави.

Як зазначає автор книги „Теорія комунікації" Г. Почепцов, як для демократичного, так і для будь-якого іншого сучасного суспільства інформаційна картина світу (уявлення про світ) важливіша, ніж сам реальний світ. Ще більшого значення набуває довгостроковий вплив ЗМІ, який є одним з основних джерел формування системи соціально-політичних настанов та стереотипів. Такі стереотипи не рідко створюються і використовуються як інструмент політичної боротьби, але саме вони можуть стати у нагоді у суспільстві, що розвивається, підтримуючи цілісність національної символьної системи (національної культури), або, при невдалому використанні, зруйнувати її. Відомо, що навіть нетривале послаблення дії національної символьної системи призводить до порушення гармонії комунікації у суспільстві. Саме тому одним з головних напрямів захисту інформаційного простору є захист національної системи символів (8; 47). У тому, що відбувається тоді, коли цей захист здійснюється невдало,' або недостатньо ми можемо переконатись на прикладі України, а саме таких «проблемних» регіонів як Донбас та АР Крим, де серед населення формується ненаціональна інформаційна картина світу.

Вважається, що надійно захистити інформаційний простір може лише така символьна система, яка здатна якнайширше розповсюджуватись, аж доки вона не втратить своєї привабливості. Відсутність відомостей про країну у світовому інформаційному просторі, або їх негативний характер, не найкращим чином впливає на зовнішньополітичну діяльність держави, а також на діяльність окремих її громадян. Саме це обґрунтовує необхідність запровадження четвертої групи заходів по підтримці інформаційної безпеки, які сприяли б поширенню присутності України у світовому інформаційному просторі. Події помаранчевої революції посприяли поширенню відомостей про Україну, а також формуванню її іміджу як демократичної країни, проте вони носили тимчасовий характер. Необхідна наявність виваженої державної стратегії у даному напрямку, щоб закріпити досягненні результати, та просунутись далі.

Враховуючи все перелічене вище, можна зробити висновок, що стан забезпечення інформаційної безпеки в Україні є задовільним, хоча існує певна низка проблем у таких сферах як забезпечення інформацією населення та державних установ, захист національного інформаційного простору, а також у сфері розповсюдження інформації про Україну, забезпечення її присутності у міжнародному інформаційному просторі. Перспективним напрямком співробітництва у сфері інформаційної безпеки є євроатлантичний напрямок, що сприятиме переходу України на нові стандарти безпеки, застосуванню нових методик та технологій, що зроблять нашу державу менш вразливою. Співробітництво з євроатлантичними структурами сприятиме також поширенню відомостей про Україну у світовому інформаційному просторі так само, як і формуванню позитивного іміджу України на світовій арені (9; 67).

Формування і реалізація єдиної державної політики по забезпеченню захисту національних інтересів від загроз в інформаційній сфері, прийняття відповідних законодавчих актів, координація діяльності органів державної влади по забезпеченню інформаційної безпеки послідовно сприятимуть приведенню української національної системи інформаційної безпеки у відповідність зі світовими стандартами у даній сфері.

ЛІТЕРАТУРА

1. Дмитрієва К. Україна - НАТО: співробітництво в галузі безпеки інформації http//www.lntersecurity.jrg/arhivst26.html.
2. Закон України „Про концепцію національної програми інформатизації" від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. - 1998. - № 27-28. - ст. 182.
3. Закон України „Про національну програму інформатизації" від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. - 1998. - № 27-28. - ст. 181.
4. Закон України „Про основи національної безпеки України" від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. - 2003. - № 39. - ст. 351.
5. Литвиненко О.В., Бінько І.Ф., Потіха В.М. Інформаційний простір як чинник забезпечення національних інтересів України.-К: „Чорнобильінтерінформ", 1998,47 с.
6. Панарин А.С. Інформационньїе политические технологии в условиях открытого общества // Кентавр. - 1994. - №2, С. 30.

7. Постанова Верховної Ради України „Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні" від 1 грудня 2005 року // Відомості Верховної Ради України. - 2006. - № 15.
8. Почепцов Г.. Теория коммуникации. - М.:Рефл-бук, 2001.
9. Тероризм і національна безпека. - http://marchuk.kiev.ua/ua/94p.html.
10. Указ Президента України „Про Стратегію національної безпеки України" від 12 лютого 2007 року № 105/20.