

Електронне наукове фахове видання "Державне управління: удосконалення та розвиток" включено до переліку наукових фахових видань України з питань державного управління (Наказ Міністерства освіти і науки України від 06.11.2014 № 1279)

ДЕРЖАВНЕ УПРАВЛІННЯ
удосконалення та розвиток



№ 8, 2014 [Назад](#) [Головна](#)

УДК 351.86: 004.056

В. В. Антонюк,
аспірант кафедри національної безпеки,
Національна академія державного управління при Президентові України, м. Київ

МЕХАНІЗМИ ДЕРЖАВНОГО РЕАГУВАННЯ НА СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

V. V. Antonyuk,
postgraduate student, The National Security Department,
The National Academy for Public Administration under the President of Ukraine

STATE MECHANISMS TO RESPOND TO MODERN CHALLENGES AND THREATS TO INFORMATION SECURITY

Розглянуто цілі та завдань механізмів державного реагування на сучасні виклики та загрози інформаційній безпеці, окреслені напрями їх вдосконалення. Зазначено, що у сучасній науці відсутнє комплексне дослідження недержавної системи безпеки як громадського механізму та громадських об'єднань як суб'єктів забезпечення національної безпеки держави. Представлено низку проблемних питань щодо функціонування та розвитку даних механізмів на сучасному етапі розвитку системи національної безпеки. Дається авторське бачення шляхів удосконалення системи адміністративно-правового регулювання інформаційної безпеки та запропоновано конкретні пропозиції щодо їх впровадження у державно-управлінську практику.

The goals and objectives of the mechanisms of response to modern challenges and threats to an information security are searched, directions to improve that mechanisms are outlined. It is noted that modern science has no comprehensive study of non-state security system as a public mechanism and public associations as subjects of the national security. A number of issues concerning the elaboration and operation of these mechanisms at the present stage of the national security system development are presented. The author's vision of improving the system of administrative and legal regulation of information security is given, the specific suggestions for implementation of the public-management practices are offered.

Ключові слова: *виклик, загроза, інформаційна безпека, механізми державного реагування, система національної безпеки.*

Keywords: *challenges, threats, information security, mechanisms of state regulation, national security system.*

Актуальність і постановка проблеми. Державне управління забезпеченням інформаційної безпеки є однією з важливих функцій держави. Його сутність полягає в забезпеченні скоординованої національної стратегії на державному, регіональних і локальних рівнях при взаємоузгодженому розподілі обов'язків нормативно-правового, інформаційного, морально-психологічного, документальних його і ресурсного забезпечення. З боку держави необхідно постійно здійснювати співставлення загроз і небезпек із наявними ресурсами щодо управління ними. Потрібна всебічна деталізація прав, обов'язків, повноважень і відповідальності усіх складових системи управління національною безпекою.

На жаль слід констатувати, що у наслідок неналежного правового регулювання в національному інформаційному просторі України спостерігається низка негативних явищ, які створюють реальні та потенційні загрози інформаційній безпеці людини і громадянина, суспільства і держави.

У 2014 році на території Автономної Республіки Крим та південно-східних регіонах України здійснювався інформаційно-психологічний тиск на населення України з боку засобів масової інформації Російської Федерації, спостерігалася інформаційна експансія в національний інформаційний простір України, захоплювались стратегічні об'єкти української телекомунікаційної інфраструктури.

За даними громадської організації «Інститут масової інформації», за період з 1 березня до 10 червня 2014 року в Україні було зафіксовано 368 фактів порушень свободи слова, з них майже 80% пов'язані з діями терористів, російською агресією, і сталися на Сході та в Криму[4]. Мали місце численні перешкодження професійній діяльності журналістів. Все це відбувається на тлі масованого і агресивного інформаційного наступу російської пропаганди, яка всупереч європейським стандартам у сфері засобів масової інформації намагалася розпалювати в Україні міжнародну ворожнечу та сепаратистські настрої, посягала на державний суверенітет і територіальну цілісність України. За цих умов актуальним постає питання вдосконалення вітчизняної системи забезпечення інформаційної безпеки в цілому, та механізмів державного реагування на сучасні виклики та загрози інформаційній безпеці зокрема.

Аналіз останніх досліджень і публікацій. Вивченню різних аспектів формування інформаційної політики держави та забезпечення її інформаційної безпеки присвячені роботи українських вчених М.М. Биченка, В.М. Бегми В.П. Горбуліна, Б.О. Демидова, Я.М. Жаркова, І.В. Замаруєва, О.В. Литвиненка, Р.Р. Марутян, М.А. Ожевана, Г.Г. Почепцова, А.О. Рось, В.Б. Толубка, С.А. Чукот, В.М. Шемаєва та інших. Проблеми формування законодавства у сфері регулювання відносин інформаційної сфери, інформатизації, захисту інформації, створення та використання інформаційних ресурсів України присвячені розробки І.В. Арістової, В.М. Брижка, В.Д. Гавловського, В.В. Грищенко, М.В. Гуцалоюка, Р.А. Калюжного, Б.А. Кормича, О.В. Кохановської, П.В. Мельника, В.С. Цимбалюка, В.О. Шамрая, М.Я. Швеця, Ю.В. Яцишина та ін. Праці названих науковців створили методологічне підґрунтя для системного розгляду переважної більшості проблем у сфері інформації та державного управління. Аналіз історіографії даного питання призводить до констатації факту, що у вітчизняній і зарубіжній літературі недостатньо розробленими залишаються питання що пов'язані саме розвитком законодавчих та правових норм і механізмів забезпечення інформаційної безпеки держави; проблеми реагування на сучасні виклики та загрози інформаційній безпеці, механізми їх формування та розвитку.

Постановка цілей. У межах цієї статті маємо за мету сформулювати уявлення щодо цілей та завдань механізмів державного реагування на сучасні виклики та загрози інформаційній безпеці, визначити напрями їх вдосконалення.

Вклад основного матеріалу. Визначаючи місце інформаційної безпеки в системі діяльності держави щодо виконання своїх функцій слід зважати на те, що на сучасному етапі виникає необхідність розглядати в комплексі предмет і зміст діяльності держави та засоби і способи, що її забезпечують, тобто досліджувати державну політику. Державна політика визначає зміст державної діяльності, способи її організації. Саме політика передбачає гармонізацію інтересів держави з

інтересами інших держав, соціальних груп та індивідів, і головне – визначення конкретного змісту та форм діяльності держави в тій чи іншій сфері.

Разом з тим, сама по собі політика є надправовою категорією і звідси регулюється правовими нормами лише у своєму зовнішньому, формалізованому виразі. Але конкретний зміст державної політики представляє собою волю держави, спрямовану на досягнення конкретної мети. Ця воля держави закріплюється у правових нормах, здійснюється за їх допомогою у процесі діяльності державних органів та інститутів. Таким чином, з правової точки зору існує певний механізм формування і реалізації державної політики, в сфері інформаційної безпеки – це організаційно-правовий механізм інформаційної безпеки.

Організаційно-правовий механізм інформаційної безпеки - це впорядкована сукупність інститутів держави, задіяних у процесі формування і впровадження політики інформаційної безпеки, внутрішні та зовнішні ролі і відносини якої регулюються системою правових норм та принципів. Цей організаційно-правовий механізм, у відповідності з означеними напрямками реалізації політики інформаційної безпеки, складається з трьох взаємопов'язаних елементів.

По-перше, це сукупність державних інститутів задіяних у процесі формування і впровадження політики інформаційної безпеки, тобто інституціональний механізм інформаційної безпеки.

По-друге, це сукупність ролей та відносин, яка включає правові відносини що виникають при проведенні політики інформаційної безпеки та специфічні ролі, форми і методи діяльності суб'єктів проведення політики інформаційної безпеки.

По-третє, це ієрархічна сукупність правових норм та принципів, що регулюють зміст та процес проведення політики інформаційної безпеки, тобто правовий механізм інформаційної безпеки. Останні два елементи складають правовий механізм інформаційної безпеки.

Сукупність інститутів публічної влади та інститутів громадянського суспільства, задіяних у процесі формування і реалізації політики інформаційної безпеки, складає інституціональний механізм інформаційної безпеки. Ієрархічна сукупність правових норм та принципів, яка регулює зміст та процес проведення політики інформаційної безпеки, а також сукупність ролей та відносин, яка включає правові відносини, що виникають при проведенні політики інформаційної безпеки та специфічні ролі, форми і методи діяльності суб'єктів проведення політики інформаційної безпеки складають правовий механізм інформаційної безпеки. Ефективність захисту інформаційної безпеки держави в цілому забезпечується ефективністю кожної складової її механізму.

Суб'єктами забезпечення інформаційної безпеки України слід вважати систему державних і недержавних інститутів, а також громадян України об'єднаних спільною метою щодо захисту національних інтересів в інформаційній сфері. Отже, коло суб'єктів забезпечення інформаційної безпеки України представляє собою багаторівневу систему, що має спільну мету – забезпечення інформаційної безпеки України, але різні повноваження, можливості, засоби тощо. До цих суб'єктів можна віднести:

- державу, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки;
- громадян, суспільні або інші організації і об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства України.

Це дозволяє стверджувати, що СЗБ перетинається із системою суб'єктів, які здійснюють інформаційний вплив. Конче важливою для функціонування цих систем є саме площина перетину інтересів. Перевага в інформаційному протистоянні залежить від того, на чий бік перехиляться терези приватного сектору.

Система суб'єктів щодо забезпечення інформаційної безпеки має працювати незалежно від внутрішньополітичної кон'юнктури в Україні та стану окремих її елементів. Системним, інтегруючим чинником має бути спільна мета для діяльності вказаних на схемі суб'єктів – забезпечення національного інформаційного суверенітету.

Отже, для подальшого усвідомлення проблеми виявлення ознак загроз національній безпеці в інформаційній сфері можна виділити перелік тих суб'єктів, які займаються процесами виявлення, оцінки інформаційних загроз та організовують проведення заходів щодо протидії. Зокрема до цього переліку можна віднести такі суб'єкти:

1. Президент України, який очолює Раду Національної безпеки і оборони (РНБО) України. Президенту України також підпорядковуються: Національний інститут стратегічних досліджень. Апарат РНБО України координує діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України та зазначених науково-дослідних установ стратегічного рівня.

2. Кабінет Міністрів України. У складі Секретаріату Кабінету Міністрів України діє Управління стратегії розвитку інформаційних ресурсів та технологій.

Основними органами Кабінету Міністрів України, що відповідають безпосередньо за інформаційну сферу є:

- Державний комітет телебачення та радіомовлення;
- Державний департамент інформатизації;
- Національна комісія з питань регулювання зв'язку.

Крім того Кабінетом Міністрів України координується діяльність:

- Державного департаменту інтелектуальної власності Міністерства освіти та науки України;
- Державної адміністрації зв'язку Міністерства транспорту та зв'язку України;
- Департаменту Державної служби боротьби з економічною злочинністю Міністерства внутрішніх справ України. У складі цього департаменту діє

Управління боротьби з правопорушеннями у сфері інтелектуальної власності та високих технологій;

- дипломатичних представництв, консульських установ та інших структурних підрозділів Міністерства закордонних справ України;
- спеціальних підрозділів Міністерства оборони і Збройних Сил України.

3. Служба безпеки України.

4. Державна служба спеціального зв'язку та захисту інформації України.

5. Розвідувальні органи України.

Зазначені вище центральні органи державного управління в ході реалізації функцій щодо виявлення загроз інформаційній безпеці держави можуть залучати ОДВ та МС, засоби масової інформації, політичні партії та рухи, громадські організації та професійні спілки, неурядові дослідницькі організації, а також інші організації та установи, що здійснюють діяльність в інформаційній сфері.

У Законі України «Про основи національної безпеки України» виписано низку основних функцій суб'єктів забезпечення національної безпеки України, які досить часто дублюються в положеннях про державні органи системи забезпечення інформаційної безпеки [2]. Це твердження є актуальним і для тих державних органів, які можна включити до складу функціональної групи оперативного виявлення інформаційних загроз та організації відповідної протидії. Основною функцією цих ОДВ є моніторинг засобів масової інформації в своїх інтересах, але при цьому не передбачено виконання завдань з виявлення відповідних небезпек та появи ознак інформаційних загроз, а тим більше відстеження динаміки їх змін, спрямованості, характеру та факту переростання в загрозу інформаційній безпеці держави.

На сьогодні прогресивним кроком є визначення Президентом України порядку щорічного уточнення військовим та спеціальним органам державного управління пріоритетних завдань із забезпечення національної безпеки України. Передбачено й відповідні форми звітності про виконання зазначених завдань, які надаються в визначені терміни до Апарату РНБО України. Протягом 2012-2013 років у Верховній Раді України було зареєстровано 3 законопроекти щодо кібернетичної безпеки України: розроблений Міністерством внутрішніх справ законопроект України "Про внесення змін до Закону "Про основи національної безпеки України щодо кібернетичної безпеки", поданий групою народних депутатів законопроект "Про кібернетичну безпеку", поданий народним депутатом Держкачем проект Закону "Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки". Цим законопроектом передбачається визначити правові та організаційні засади забезпечення кібернетичної безпеки України, основоположні принципи державної політики у сфері кібернетичної безпеки, національної системи кібербезпеки, а також повноваження суб'єктів забезпечення кібербезпеки

Нарешті, у відповідь на виклики, які сьогодні стоять перед Україною, Указом виконуючого обов'язки Президента від 1 Травня 2014 року № 449 затверджено та введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»[5].

В цілому, механізм інформаційної безпеки повинен включати цілу низку різних владних інститутів, які тим або іншим чином здійснюють узгоджену комплексну діяльність в інформаційній сфері. Разом з тим слід відмітити, що було б абсолютно помилковим зводити цей механізм виключно до системи державного управління.

Забезпечення національної безпеки держави – це справа не тільки органів державної влади, а й усього суспільства і кожного громадянина. Наявність ефективної мережі громадських структур стає за сучасних умов однією з умов забезпечення національної безпеки. Відповідно до Закону України «Про основи національної безпеки України» громадяни України, об'єднані громадян є суб'єктами забезпечення національної безпеки, а розвиток громадянського суспільства, його демократичних інститутів визнано пріоритетним напрямом реалізації національних інтересів України[2].

Однак, наука в Україні до цього часу комплексно не досліджувала недержавну систему безпеки як громадський механізм, а громадські об'єднання – як суб'єкти забезпечення національної безпеки держави. Діяльність окремих різновидів громадських об'єднань не пов'язувалася з державною стратегією забезпечення національної безпеки.

В Україні недержавна система забезпечення національної безпеки перебуває на стадії формування і не має істотного впливу на ситуацію. Сьогодні їй бракує єдиного координуючого органу як методичного та організаційного центру. В цьому контексті актуальними можна вважати пропозиції щодо організації при РНБО України Центру недержавного забезпечення національної безпеки України або Незалежної громадської консультативної ради з представників українського і міжнародного експертних співтовариств.

Проблему забезпечення інформаційної безпеки необхідно розглядати в загальнодержавному вимірі. У державному механізмі забезпечення інформаційної безпеки мають бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів виявлення та нейтралізації загроз. Він обов'язково має включати двосторонній зв'язок між суспільством, ЗМІ й державою, який допоможе своєчасно сповістити про зміни громадської думки під цілеспрямованим впливом та оцінювати ефективність заходів з протидії.

Для реалізації зазначених положень необхідна чітка система органів, яка може перебрати на себе завдання із захисту інформаційного простору. В своїх дослідженнях та наукових висновках український вчений В.В. Остроухов наголошує саме на формальному існуванні такої системи та виділяє чотири взаємопов'язані її рівні: законодавче забезпечення та парламентський контроль здійснюються Верховною Радою України; правоохоронна функція, функція забезпечення національної безпеки забезпечується рядом органів, підпорядкованих Президенту України; управлінські, адміністративні функції зосереджуються в Кабінеті Міністрів України; приватна ініціатива, комерційний інтерес та громадський контроль реалізуються через діяльність різноманітних недержавних організацій та незалежних ЗМІ [1;3].

В цілому, аналіз стану забезпечення інформаційної безпеки показує необхідність удосконалення системи адміністративно-правового регулювання інформаційної безпеки. Постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторинг інформаційного середовища, наявності загроз та небезпек.

Удосконалення системи державного реагування на сучасні виклики та загрози інформаційній безпеці потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів. Все це дає можливість стверджувати, що система забезпечення інформаційної безпеки має бути міжвідомчою і ієрархічно організованою, її структура і організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів.

Організація ефективного державного реагування на сучасні виклики та загрози інформаційній безпеці передбачає централізоване управління із конкретними відомчо-розпорядничими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоспектрної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування.

Виходячи з всього вищезгаданого, доходимо до таких висновків.

На сучасному етапі розбудови системи інформаційної безпеки виняткове значення має зміцнення нормативно-правової бази функціонування інформаційного середовища в цілому та проблеми забезпечення інформаційної безпеки. Динамізм відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені регулятори суспільних відносин, ускладнює створення стабільної правової регламентації. Відставання, недосконалість нормативно-правової бази дозволяє окремим суб'єктам реалізовувати свої протиправні наміри і можливості в інформаційній сфері щодо широкого спектра інтересів інших як суб'єктів, так і об'єктів національної безпеки.

Безперечним є необхідність удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері. При чому важливою є не стільки статика окремих нормативно-правових актів, скільки динаміка доповнень, яка б містила механізми генерації нових рішень, проектів, що дозволяють діяти в темпі, які диктує інформаційне суспільство.

Україна потребує такі нормативно-правові акти, які б упорядковували відносини з формування і ведення інформаційних ресурсів державного, регіонального і локального рівнів. Актуальним є нормативне закріплення орієнтації державних і суспільних інформаційних ресурсів на діяльність органів державного управління. Також потребують вирішення проблеми правового регулювання інформаційних технологій, які створюють інфраструктуру інформаційного суспільства, питання інтелектуальної власності в сфері інформаційних відносин. Необхідні нормативно-правові акти, які б регулювали суспільні відносини в сфері обліку та моніторингу в інформаційній сфері.

Слід законодавчо встановити затверджені положення: про обов'язковий склад і основну технічну комплектацію виробничих і корпоративних мереж, які впливають на стан інформаційної безпеки; про обов'язкові вимоги по інформаційній безпеці систем, програмного і апаратного забезпечення; про безпечне ведення бізнесу із використанням нових інформаційних технологій і глобальних інформаційних мереж.

Потребують подальшого вирішення питання щодо розробки інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвиток системи сертифікації інформаційних продуктів, систем і послуг; створення системи ліцензування діяльності організацій по окремих напрямках формування єдиного інформаційного простору України.

Перспективи подальших досліджень. Викладені результати дослідження частково окреслюють проблемне поле функціонування системи забезпечення інформаційної безпеки України. У подальшому автор вважає доцільним дослідити зарубіжний та вітчизняний досвід щодо взаємодії державних та недержавних суб'єктів при розробці та впровадженні політики забезпечення інформаційної безпеки.

Література.

1. Закон України «Про захист персональних даних» // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 1188.
2. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.
3. Коментар до проекту Доктрини інформаційної безпеки України [Електронний ресурс]. – Режим доступу: <http://www.rainbow.gov.ua/news/942.html>
4. Підсумки порушень прав журналістів та свободи слова з початку російської агресії – IMI (інфографіка). – Режим доступу: <http://imi.org.ua/analytics/44669-pidsumki-porushen-prav-jurnalistiv-ta-svobodi-slova-z-pochatku-rosijskoji-agresiji-imi-infografika.html>
5. Указ Президента України № 449/2014 Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" [Електронний ресурс]. – Режим доступу: <http://www.president.gov.ua/documents/17588.html?PrintVersion>

References.

1. The Verkhovna Rada of Ukraine (2010), "Zakon Ukrainy "Pro zahyst personal'nyh danyh", Vidomosti Verhovnoi' Rady Ukrainy, vol. 34, p. 1188.
2. The Verkhovna Rada of Ukraine (2003), "Zakon Ukrainy "Pro osnovy nacional'noi' bezpeky Ukrainy", Vidomosti Verhovnoi' Rady Ukrainy, 2003, vol. 39, p. 351.
3. Komentar do proektu Doktryny informacijnoi' bezpeky Ukrainy [Elektronnyj resurs], Rezhym dostupu: <http://www.rainbow.gov.ua/news/942.html>
4. Pidsumky porushen' prav zhurnalistiv ta svobody slova z pochatku rosijs'koi' agresii', IMI (infografika). Rezhym dostupu: <http://imi.org.ua/analytics/44669-pidsumki-porushen-prav-jurnalistiv-ta-svobodi-slova-z-pochatku-rosijskoji-agresiji-imi-infografika.html>
5. Ukaz Prezidenta Ukrainy vol. 449/2014 Pro rishennja Rady nacional'noi' bezpeky i obrony Ukrainy vid 28 kvitnja 2014 roku "Pro zahody shhodo vdoskonalennja formuvannja ta realizacii' derzhavnoi' polityky u sferi informacijnoi' bezpeky Ukrainy" [Elektronnyj resurs]. Rezhym dostupu: <http://www.president.gov.ua/documents/17588.html?PrintVersion>

Стаття надійшла до редакції 20.08.2014 р.



ТОВ "ДКС Центр"