Максимець В.Є.*

КОНЦЕПТУАЛЬНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЛОВАЦЬКОЇ РЕСПУБЛІКИ

У даній статті проаналізовано основні проблеми формування системи інформаційної безпеки Словацької Республіки та роль держави в цьому процесі, а також шляхи подолання цих проблем.

Ключові слова: Словацька Республіка, інформаційна безпека, інформаційні та комунікаційні технології.

В данной статье проанализированы основные проблемы формирования системы информационной безопасности Словацкой Республики и роль государства в этом процессе, а также пути преодоления этих проблем.

Ключевые слова: Словацкая Республика, информационная безопасность, информационные и коммуникационные технологии.

This article analyzes the main problems of the Slovak Republic information security system and the state's role in this process, and ways to overcome these problems.

Key words: the Slovak Republic, information security, information and communication technology.

Актуальність дослідження та постановка проблеми. Розвиток суспільства залежить від інформаційно-комунікаційних технологій, оскільки вони суттєво впливають як на внутрішню, так і на зовнішню політику держави. В даний час через інформаційні та комунікаційні системи інформаційно-комунікаційної інфраструктури, проводяться операції практично у всіх сферах життя (фінанси і банківська справа, енергетика, телекомунікації, охорона здоров'я і соціальне забезпечення, оборони, безпеки, освіти, культури, звичаїв та ефективності державного управління і т.д.) [1]. Необхідна умова функціонування суспільства – це інформаційна безпека в країні. У широкому сенсі це означає забезпечення інформаційної безпеки та захисту інформаційного простору і зокрема захисту інформаційно-комунікаційної інфраструктури держави та її інформаційний зміст, які відносяться до концепції стратегії в цифровому просторі.

Поняття інформаційної безпеки, з одного боку, може розглядатись як захищеність внутрішньої інформації як такої, що припускає захищеність якості інформації, її надійність, захищеність різних галузей інформації (державної, банківської, комерційної таємниці) від розголошення. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою, захист національного інформаційного простору від зовнішньої інформаційної експансії [2, p.16].

* асистент кафедри міжнародної інформації Національного університету «Львівська політехніка»

© Максимець В. Є., 2011

Інформаційна безпека держави – це стан її інформаційної захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютерні злочини не завдають суттєвої шкоди національним інтересам.

Категорія національних інтересів в інформаційній сфері в повній мірі узгоджується з іншою категорією – національною безпекою, і співвідноситься між собою за схемою «частина» і «ціле». При цьому слід враховувати, що інформаційна складова не може існувати поза цілями загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки.

У цілому політика національної безпеки Словацької Республіки спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку держави у відповідності з її цілями. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством. Ось чому питання формування інформаційної безпеки є надзвичайно важливими й актуальними в аналізі стану справ у цій галузі, оскільки інформаційна безпека є складовою частиною національної безпеки. Вивчення імперативів концепції інформаційної безпеки Словацької Республіки дозволить показати найбільш перспективні напрямки удосконалення діяльності держави для запобігання погроз, що несе із собою некерована інформаційна революція. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

Обрана проблематика має політичну науково-теоретичну та практичну цінність, виконана в межах напряму кафедри міжнародної інформації НУ «Львівська політехніка» «Моделювання міжнародних інформаційних потоків» та кафедральної тематики: «Аналіз інтеграції європейських посткомуністичних держав в ЄС та НАТО: досвід для України» (номер державної реєстрації – МІ – 1 0109U003464).

Аналіз останніх досліджень та публікацій з цієї проблеми свідчить, що вона є предметом дослідження багатьох українських науковців. Так, з'являються публікації українських фахівців у цій сфері, зокрема Л. Янчук аналізувала зовнішню політику Словацької Республіки, В. Парфенюк досліджував особливості розвитку та зміст політики інформаційного суспільства в умовах євроінтеграції в країнах Центральної Європи.

Мета статті – розкрити основні засади формування інформаційної безпеки Словацької Республіки, а також обґрунтувати найбільш ефективні способи використання інформаційних технологій, місця і ролі інформаційної політики держави в цій галузі. Завдання дослідження відповідно охоплюють аналіз інформаційної безпеки в структурі інформаційної політики Словацької Республіки.

Виклад основного матеріалу. Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки [3, с. 28].

Останнє десятиліття в історії Словаччини характеризувалося низкою радикальних трансформацій, серед яких перехід до ринкової економіки, інтеграція в ЄС. Одним із найважливіших пріоритетів у розвитку інформаційної безпеки в Словаччині стала модернізація інформаційних систем, комп'ютеризація державних установ та вдосконалення

доступу до державної інформації. Основна активність уряду Словацької Республіки щодо розвитку інформаційної політики припадає на початок нового століття, коли стала реальною перспектива вступу до ЄС. Формування комплексної політики розпочалось з того, що протягом декількох років Словаччина детально розробляла загальний національний план інформаційної безпеки, який потім модифікувався згідно з вимогами з ЄС.

Важливість інформаційної безпеки починають розуміти національні уряди, наднаціональні органи та організації розвинених країн у світі (ООН, G8), створюються різні установи та інституційні системи для забезпечення захисту інформації (ENISA HLIG, CERT, та інші.). У зв'язку з цим у березні 2004 р. було створено Європейське агентство з інформаційної безпеки – ENISA, яке об'єднує всі держави-члени ЄС, де Словацьку Республіку представляє Міністерство фінансів.

На Лісабонському саміті в 2000 р., глави держав і урядів погодилися з тим, що ЄС «до 2010 року стане найбільш конкурентоспроможним та динамічним, здатним до стійкого зростання» та затвердили стратегію e-Europe, яка в 2005 р. була замінена на «І-ініціатива-2010» (Європейське інформаційне суспільство 2010 р.) [4, с. 5]. До основних пріоритетів ЄС включив питання інформаційної безпеки та приступив до здійснення ряду стратегічних документів, рекомендацій, керівних принципів і правил, що стосуються конфіденційності та комп'ютерних програм, електронних підписів, електронної торгівлі, боротьби з кіберзлочинністю, боротьби зі спамом і так далі. Тому для підтримки інформатизації був розроблений проект «Електронна Словаччина», оприлюднена 30 квітня 2002 р., цілями котрого стали розширення інтернет-доступу та доступності електронних послуг для населення, підвищення якості змісту, поліпшення освіти і навчання населення в оволодінні комп'ютерами та Інтернет.

У період після вступу до ЄС Словаччина мала певні труднощі щодо реалізації своєї стратегії інформаційної безпеки. До 31 грудня 2008 р., виконання завдань, визначених в Плані дій контролювалося на безперервній основі (відкрита природа плану давала змогу доповнювати його новими завданнями, оскільки потреби окремих секторів розвивалися). Негативні аспекти полягали в тому, що план містив низку дуже загально сформульованих завдань без конкретних фінансових асигнувань, як наслідок, деякі завдання не були виконані взагалі, а інші виконувалися частково, або із затримкою [5, с. 217].

Базовим документом в сфері інформаційної безпеки Словацької Республіки є «Національна стратегія інформаційної безпеки», прийнята урядом Словаччини 27 серпня 2008 р. Враховуючи, що інформаційна безпека вимагає комплексного підходу необхідно визначити її базовий рівень, можливість розширення в конкретних областях. Правильне визначення інформаційної безпеки має важливе значення для створення первинних законодавчих норм у цій області, а також наступним етапом до вирішення проблеми інформаційної безпеки в Словаччині.

Стратегія включає основні напрями, пріоритети та заходи для досягнення цілей. Документ також загально описує кожне завдання для забезпечення захисту всього віртуально-інформаційного простору Словацької Республіки, що стосується національної безпеки. Це включає, зокрема заходи проти витоку інформації і несанкціонованого використання, порушення цілісності даних, порушення прав громадян на недоторканність приватного життя, захист від ушкоджень і використанням інформаційних та комунікаційних систем, наклеп державних і приватних установ, а також заходи щодо забезпечення дотримання законів Словацької Республіки та Європейського союзу. Недостатній рівень захисту інформації та інформаційно-комунікаційних технологій призводить до підриву інформації довіри і впевненості доступу з Інтернету, які в даний час має мережа взаємо-

пов'язаних комп'ютерних систем у більш ніж 250 країнах світу. Ця найбільша мережа в світі сьогодні пропонує доступ до практично необмежених джерел інформації, дозволяє її обміну і надає велику кількість послуг, таких як електронна пошта, передача файлів і т.д. З цих причин, надійної роботи інформаційних систем, надійного обміну інформацією та пов'язані з інформаційною безпекою є ступінь гарантії безпеки, основних прав і свобод громадян та розвитку конкурентоспроможності кожної країни. Саме «Національна стратегія інформаційної безпеки» в Словаччині допомагає підвищити довіру до електронних послуг, електронної торгівлі, конкурентоспроможності [6].

Висновки та перспективи подальших досліджень. Державна політика забезпечення інформаційної безпеки Словацької Республіки – це надзвичайно важливе завдання, що повинно вирішуватись в ході здійснення реформування суспільства. Метою такої політики повинно бути, насамперед, створення умов для своєчасного виявлення джерел інформаційних погроз і можливих їхніх наслідків. Необхідно визначити комплекс превентивних мір з метою нейтралізації або зменшення негативних наслідків інформаційних погроз, створити умови для забезпечення своєчасної, повної і точної інформації для прийняття рішень, здійснювати інформаційну діяльність з метою гармонізації особистих, суспільних і державних інтересів як основи досягнення політичної стабільності в суспільстві.

Література

1. Informačná bezpečnosť [Електронний ресурс]. – Режим доступу: http://www.informatizacia.sk/informacna-bezpecnost/2999s.
2. Thomas R. Peltier, J. Peltier, J. Blackley Information security. - Washington: Auerbach, 2005. – 228 p.
3. Правові основи інформаційної діяльності: Навч. посібник / С. Ф. Гуцу. – Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін-т», 2009. – 48 с.
4. Парфенюк В.М. Політика інформаційного суспільства в умовах євроінтеграції (на прикладі Республіки Польща, Словацької Республіки, Угорської Республіки та Чеської Республіки): автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку»/В.М. Парфенюк; Ін-т світової економіки і міжнар. відносин НАН України.–К., 2006. – 18 с.
5. Парфенюк В. М. Трансформація політики країн Вишеградської групи в сфері інформаційно-комунікаційних технологій в період 2000-2010 років / В.М. Парфенюк // Слов'янський вісник: збірник наукових праць. Серія «Історичні та політичні науки» / Рівненський інститут слов'янознавства Київського славістичного університету. – 2011. – Вип. 11. – С. 213-220.
6. Národná stratégia pre informačnú bezpečnosť v SR [Електронний ресурс]. – Режим доступу: http://www.informatizacia.sk/národná-stratégia-pre-ib/6783s