УДК 338.24

Фесенко А.Б., студент; Лахижа М.І. д.н.держ.упр., професор
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПОСТСОЦІАЛІСТИЧНИХ КРАЇНАХ ЄС

Постсоціалістичні країни — це держави, які здійснюють перехід від планової до ринкової економіки. Більшість таких країн виникла в кінці 80-х – на початку 90-х років в результаті розвалу соціалістичної системи управління. Значна частина цих країн увійшла до складу Європейського Союзу [1].

Аналізуючи підходи до забезпечення інформаційної безпеки, прийняті в країнах Європи, можна дійти висновку, що на сьогодні не існує уніфікованої моделі побудови національної системи безпеки в цій сфері. Втім, потреба реалізації ефективних заходів із протидії сучасним загрозам інформаційній безпеці зумовлює потребу у вдосконаленні форм і методів захисту інформації всіма без винятку європейськими країнами.

Ще в 1991 році на теренах Європи було сформовано ключові складові інфобезпеки - «Європейські критерії безпеки інформаційних технологій». Ними окреслені шляхи та напрями підтримки інформаційної безпеки: протидія несанкціонованого доступу та модифікації ІТ-систем, гарантія їх цілісності, захист та підтримка працездатності інформаційних мереж шляхом перешкоджання можливих загроз відмови та проблем в обслуговуванні.

Республіка Польща. Національна інформаційна політика Польщі ґрунтується на засадах заснування незалежної відкритої спільноти, гарантуванні прав громадян, формування дієвої стратегії вільного транскордонного обміну інформацією, створення та підтримки незалежних мас-медіа. Правовим фундаментом, на якому ґрунтуються базові складові інформаційної політики, є прийняті в 90-х роках минулого століття «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща». Зважаючи на значний вплив клерикальної інформації на світогляд польської громади, особливу увагу відведено правам церкви.

Агентство внутрішньої безпеки (ABW) є основою забезпечення кібербезпеки Польщі. Про це свідчить її діяльність щодо розробки Стратегії кібербезпеки Польщі та створення Центру криптології при Міністерстві національної оборони, що забезпечує захист інформації, кібероборону та проведення наступальних кібероперацій. ABW було сформовано урядову команду реагування на комп'ютерні атаки, напрямом основної діяльності якої є захист органів державного управління від кіберзагроз ІТ-систем та комп'ютерних мереж. Під керівництвом Агенства також було розроблено й Доктрину кібербезпеки Польщі, яка визначає базові аспекти проблем інфобезпеки, зокрема «загрози», «виклики», «ризики» тощо і є виконавчим документом Стратегії національної безпеки. Активну участь в забезпеченні інформаційної безпеки Польщі приймають і громадяни країни, шляхом створення неурядової організації - Центру аналізу пропаганди і дезінформації, яка протидіє російській пропаганді [2, с. 107].

Угорщина. Політика Угорщини здебільшого характеризується впровадженням обмежень у сфері забезпечення інформаційної безпеки. Прийняття у 2010 році закону про ЗМІ викликав бурхливу критику з боку світових та європейських мас-медіа. Країну звинуватили у прагненні встановлення тоталітарного режиму, зокрема майже абсолютного контролю за ЗМІ, Інтернет-ресурсами, фактичній забороні свободи слова. Враховуючи вищезгадані обмеження, вперше до країни-члена ЄС Європейським парламентом було прийнято резолюцію щодо обмеження демократичного суспільства, прав людини та свободи слова. Незважаючи на це, парламентом Угорщини кардинальних поправок до закону внесено

не було, а лише незначні поправки, які суттєво не змінили систему управління та впливу на вітчизняні ЗМІ, при цьому викликали позитивну реакцію ЄС.

Щодо захисту персональних даних, то тут Угорщина взяла на себе роль флагмана серед усіх постсоціалістичних країн, де у 1992 році інститутом Парламентського комісара із захисту та свободи інформації був прийнятий відповідний правовий акт - «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес». Законом передбачено публікувати інформацію, обробку якої здійснюють органи, що виконують суспільні обов'язки, крім інформації про особу. На вирішення проблем інформаційних загроз у безпеці Угорщини спрямована дія Закону «Про електронну інформаційну безпеку державних та муніципальних органів», а також розроблення у 2012 році Стратегії національної безпеки Угорщини. Зазначена Стратегія регулює ризики й загрози, що можуть мати суттєвий вплив на державну безпеку, оборону, протидію кримінальному впливу та уникненню критичних обставин та інцидентів у кіберпросторі.

Чеська Республіка. Конституцією Чеської Республіки 1992 р. гарантується право на інформацію у ст. 17, де зібрані усі правові норми, що регламентують різні аспекти цього права: заборона цензури, обов'язок державних органів надавати інформацію щодо своєї діяльності та ін. Питаннями інформаційної безпеки країни Чехії займається Військова розвідувальна служба (ВРС). Служба відповідає за своєчасне інформування військово-політичного керівництва країни та партнерів по НАТО про потенційні загрози та агресивні плани держав, що знаходяться в зоні інтересів Чехії та Альянсу. Кадрові співробітники розвідслужби є військовослужбовцями за контрактом, а її діяльність повністю фінансується з бюджету військового відомства. До основних задач чеської розвідслужби належить забезпечення країни розвідувальною інформацією, організацією інформаційного протиборства, отримання даних про реалізацію міжнародних угод та інші. Але головним контррозвідувальним органом країни є Інформаційна служба безпеки (BIS). Вона являє собою самостійний державний інститут, що підпорядковується безпосередньо прем'єр-міністру і має пряме фінансування із національного бюджету. Інформаційна служба безпеки займається: забезпеченням країни інформацією про наміри та дії, спрямовані проти демократичних засад держави; забезпеченням захисту відомостей, що становлять державну таємницю; збіром та аналізом інформації про реальні та потенційні загрози, пов'язані з експлуатацією інформаційних та комунікаційних систем [3].

Висновки. Питання забезпечення гарантій інформаційної безпеки громадян, суспільства, країни та уникнення спроб кібератак однозначно є першочерговим завданням державного управління та критеріїв захисту національних інтересів світової і, зокрема, європейської спільноти, які ґрунтуються, перш за все, на стандарти ЄС та НАТО. Ці стандарти бажано використовувати і українській ІТ-сфері в рамках процесу активного входження до Євросоюзу. Також Україні доречно було б об’єднатися з провідними державами Європи з метою інтеграції системи вітчизняної інформаційної безпеки до міжнародної для уникнення можливих загроз політичної, економічної, фінансової стабільності, зокрема кібертероризму та кіберзлочинності у цих сферах. Зміцнення національної інформаційної безпеки України та захист її національних інтересів значно зросте за умов тісного співробітництва з європейськими країнами.

Список використаних джерел

1. Постсоціалістичні країни: URL: https://korotko.info/2476

2. Ткачук Т.Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. Юридичний науковий електронний журнал. №5. 2017. С. 104-110 URL: http://lsej.org.ua/5_2017/30.pd

3. Спеціальні служби Чехії: URL: http://factmil.com/publ/strana/chekhija/specialnye_sluzhby_cheshskoj_respubliki_2017/109-1-0-1128