Назар БЕРНАДА
здобувач вищої освіти 1 курсу ОС «Бакалавр»
спеціальності 201 «Агрономія»
Науковий керівник:
канд. екон. наук, доцент Ірина МУШЕНИК
Заклад вищої освіти «Подільський державний університет»
м. Кам'янець-Подільський

ОСОБЛИВОСТІ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційні технології використовуються не лише в комерційній, а й у військовій галузі. Інформаційна безпека у військовій сфері є досить традиційною сферою. Захищаються від засобів розвідки як пасивними, так і активними методами. Сьогодні одним з найістотніших об'єктів безпеки в оборонній сфері є інформаційні ресурси та структура оборонного потенціалу країни.

У сучасних військово-політичних реаліях важко і навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати війни та політичні кризи без жодного пострілу, формуючи та розпалюючи внутрішні протиріччя. Така тактика характерна для війн нового формату – гібридних, де безпосередній військовий фактор є лише однією зі складових цілого[1].

Варто звернути увагу на те, що в умовах, коли цілий комплекс інформації розрахований на маніпулювання громадською думкою, свідомістю людини та подається за допомогою фізіологічних і психологічних методів і засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження здатності людини до критичного сприйняття, стає важливим аналіз та оцінка отриманої інформації. У цьому випадку здатність до формування власної думки практично відсутня.

Цілком правильно вважати, що інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз [4].

Форми та способи забезпечення інформаційної оборони держави утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують увесь комплекс завдань із захисту життєво важливих інтересів особи, суспільства та держави. Тому необхідне чітке юридичне оформлення при

розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права у будь-якій діяльності, у тому числі політичній. Своєю чергою кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки своїх дій для інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу [2].

Головним завданням системи забезпечення інформаційної безпеки країни є створення умов для організації управління системою інформаційної безпеки. До основних завдань системи забезпечення інформаційної безпеки належать: створення умов для забезпечення інформаційного суверенітету країни; забезпечення інформаційної безпеки всіх складових елементів системи державного управління; реалізація державної політики інформаційної безпеки; виявлення, запобігання і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління [3].

Висновок. Незаперечним є той факт, що сучасні загрози інформаційній безпеці є викликом далеко за межі держави та посягають не лише на національний простір, а й мають важкі глобальні наслідки. З огляду на це, для запобігання та протидії сучасним інформаційним загрозам необхідно не лише прийняти нормативно-правову базу, а й забезпечити функціонування інституційного механізму забезпечення інформаційної безпеки. На етапі підготовки держави до оборони неабияке значення має дотримання вимог щодо збереження державної таємниці та здійснення заходів з кібероборони держави для забезпечення її обороноздатності, вжиття заходів щодо стримування та протидії загрозам інформаційній безпеці країни та нейтралізації інформаційної агресії.

Список використаних джерел

1. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. URL: https://doi.org/10.24144/2307-3322.2023.77.2.20
2. Зозуля О. С. Інституційна система державного управління інформаційною безпекою України. Сучасний стан та шляхи удосконалення. URL: http://www.investplan.com.ua/?op=1&z=4344&i=29
4. Кривцов В. Ю. Інформаційні заходи оборони держави в сучасних умовах. URL: https://doi.org/10.36695/2219-5521.1.2023.05.
5. Мушеник І. М. Організаційна трансформація діяльності сфери освіти в умовах воєнного стану / Мушеник І.М.// Інновації в сучасній освіті: методологія, технологія, дидактичні та виховні аспекти. Монографія / за заг. ред. В. В. Іванишин. Кам'янець-Подільський. Заклад вищої освіти «Подільський державний університет». Рига, Латвія: "Baltija Publishing", 2023. С. 61–71.