Томашевський О. С., слухач
Національний університет оборони України
імені Івана Черняховського, м. Київ

УМОВИ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз стану справ щодо вирішення проблеми захисту національного інформаційного простору показав, що протягом попередніх років зазначене питання привертало до себе увагу багатьох фахівців, але мало переважно теоретичний характер.

Так, у наукових роботах багатьох дослідників [1, с. 29] аналізуються причини виникнення та наявний стан системи інформаційної безпеки. Лише деякі фахівці надають пропозиції щодо шляхів та невідкладних кроків її побудови в Україні. Однак глибокого аналізу наявного стану забезпечення інформаційної безпеки (ІБ) держави і суб'єктів воєнної сфери більшість відомих робіт не містить, а ті, що є, здебільшого стосуються технічних питань, зокрема кібербезпеки.

Комплексне дослідження наявних складників системи протидії інформаційно-психологічному впливу [2, с. 38] показало, що вплив інформаційних загроз на процес імплементації національних інтересів у воєнній сфері виявив, що, на жаль, за останні роки у більшості випадків антиукраїнські інформаційні заходи Російської Федерації досягали поставленої мети. Навіть зараз, коли до інформаційного протиборства з державою-агресором активно долучилася патріотично налаштована частина громадянського суспільства, приватні видання, журналісти, блогери, ми ще багато у чому втрачаємо в цьому протиборстві через неготовність насамперед профільних державних структур до виконання завдань в умовах інформаційної війни.

Метою тез є дослідження умов створення системи інформаційної безпеки Міністерства оборони України та Збройних Сил України.

До того ж відсутність в Україні ефективних механізмів інформаційної протидії на тлі багаторічного постійного потужного негативного інформаційного впливу (ІВ) на Україну і її населення з боку РФ слід розглядати як злочинну недбалість тих органів державної влади, які зобов'язані були займатися питаннями національної ІБ. Прикро, що зроблені протягом 2015–2023 рр. кроки з формування загальнодержавної системи забезпечення інформаційної безпеки були нівельовані нищівними діями попередньої влади. Зокрема, розформування в 2010 р. Департаменту інформаційної безпеки Ради національної безпеки і оборони України та низка інших рішень попереднього державного керівництва щодо згортання функцій організації і координації заходів ІБ в нашій державі призвели до значного посилення позицій іноземних країн, насамперед Росії, в інформаційному просторі України. Внаслідок цього останніми роками російські ЗМІ мали мож-

ливість поширення в українському суспільстві антиукраїнських ідей і думок, формування в населення південно-східних регіонів і Автономної Республіки Крим проросійських настроїв.

Головною причиною невдач в інформаційному протиборстві, як вбачається, слід вважати фактичну відсутність у державі та у її ЗС дієвих систем інформаційної безпеки, які б забезпечували не тільки своєчасне виявлення та аналіз інформаційних загроз національній і воєнній безпеці, а й, що надзвичайно важливо, адекватну обстановці превентивну системну протидію цим загрозам та ведення інформаційних дій наступального характеру.

Отже, проблема створення загальнонаціональної системи забезпечення інформаційної безпеки є ключовою у питанні забезпечення надійної інформаційної безпеки нашої держави та активної інформаційної протидії російській агресії.

Водночас, відсутність сьогодні в державі центрального управлінського органу, який би визначав і ставив конкретні завдання та координував діяльність усіх суб'єктів системи забезпечення інформаційної безпеки з виявлення інформаційних загроз і протидії їм та ведення єдиної інформаційної політики. Раніше на цю функцію претендував колишній Департамент інформаційної безпеки РНБО України, але був у 2015 р. розформований. На жаль, останніми роками ситуація не покращилася.

Не готовими до активного протиборства в інформаційній сфері з державою-агресором виявилися і сили інформаційно-психологічної протидії та кібернетичного захисту ЗС України.

На початок 2014 р. в ЗС України функціонувала низка структурних підрозділів, які тією чи іншою мірою забезпечували виявлення і протидію ІЗ. Незважаючи на те, що зазначені підрозділи та їх особовий склад загалом сумлінно виконували поставлені завдання та обов'язки, ефективно протидіяли реальним ІЗ, ведення активних наступальних дій в інформаційному просторі проти держави-противника організовано не було.

Проведений аналіз показав, що основними проблемами, які перешкоджають своєчасному й ефективному реагуванню на інформаційні загрози у ЗС України, є:

– відсутність у ЗС України, як і в державі загалом, системи ІБ, яка б забезпечувала не тільки виявлення та аналіз інформаційні загрози національній безпеці, зокрема у воєнній сфері, а й, що надзвичайно важливо, адекватну обстановці протидію цим загрозам;

– відсутність управлінського органу в ЗС України, який би визначав і ставив конкретні нагальні завдання з виявлення інформаційні загрози та протидії їм і координував би діяльність усіх підрозділів, що залучені до виконання цих завдань. Як наслідок, ми сьогодні спостерігаємо відсутню відповідальність усіх структур, які задіяні в процесі забезпечення ІБ ЗС України, за незадовільний кінцевий результат інформаційного протиборства;

– відсутність чіткого механізму реалізації отриманої інформації про виявлені інформаційні загрози. Внаслідок цього розвідувальна інформація про завчасно виявлені, проаналізовані і прогнозовані загрози, що надходили на адресу керівних органів держави і ЗС України, часто залишалася поза увагою останніх. І це враховуючи те, що інформація, яку надає Головне управління розвідки Міністерства оборони України, вагома, упереджувальна, з висновками, прогнозами і пропозиціями, що неодноразово зазначалося керівниками і спеціалістами Ради національної безпеки і оборони України, Міністерства закордонних справ України, іншими споживачами розвідувальної інформації;

– необґрунтоване дублювання функцій низкою інформаційних структур з виявлення інформаційні загрози, що призводить до розпорошення їх зусиль та нераціонального використання сил і засобів;

– відсутність як у державі, так і в її ЗС достатньо підготовлених спеціалізованих підрозділів для ведення активних інформаційно-психологічних та кібернетичних дій в інформаційному просторі [3, с. 54].

Отже, усі перелічені вище обставини стали головними внутрішніми негативними чинниками, що дали змогу РФ майже безперешкодно провести цілу низку антиукраїнських інформаційних операцій, акцій і атак у межах інформаційної кампанії щодо розколу українського суспільства та встановлення контролю над південними і східними областями нашої держави.

Список використаних джерел

1. Почепцов Г. Г. Стратегічні комунікації: стратегічні комунікації в політиці, бізнесі та державному управлінні. Київ: Альтерпрес, 2008. 216 с.

2. Кушнір О. В. Поняття і сутність СК в сучасному українському державотворенні. *Право і суспільство*. 2015. № 6.

3. Терещеня О. В. Стратегічні комунікації у науково-теоретичному дискурсі. *Communications and Communicative Technologies*. 2020. Вип. 20.