УДК 342.22:351.8624
DOI: 10.31733/15-03-2024/2/324-326

Ольга КУЛІНІЧ
завідувач кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ
кандидат юридичних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення національної інформаційної безпеки є пріоритетним питанням у державі в умовах режиму воєнного стану і може бути забезпечена лише за умови ефективної взаємодії між державою та громадянським суспільством, та за участі всіх внутрішніх суб'єктів інформаційної діяльності для ефективного розвитку інформаційної сфери та спільного захисту від зовнішніх загроз.

За цих обставин при розгляді організаційних питань забезпечення інформаційної безпеки особливого значення набуває структурна класифікація організацій, відносно умовна та орієнтована на конкретні цілі та завдання.

Для належного реагування на розширення гібридних загроз в Україні наприкінці 2021 року на національному рівні прийнято Стратегію інформаційної безпеки як базовий документ, що визначає завдання та напрямки діяльності держави, спрямованої на запобігання кризовим явищам в країні [1].

Тому до переліку загроз і викликів, які стоять перед нашою державою, входять: комплексна інформаційна політика російської федерації; досить низька медіаграмотність населення; кількість глобальних кампаній з дезінформації динамічно зростає; інформаційний контроль російської федерації на тимчасово окупованих територіях; використання методів маніпулювання суспільною свідомістю щодо наслідків членства України в НАТО та ЄС.

Зокрема, за умови успішної реалізація стратегії інформаційної безпеки планується мати такі позитивні результати, як створений захищений інформаційний простір, який гарантує безпеку інформації, гарантовану нації та її виборцям; ефективне функціонування системи стратегічних комунікацій.

В умовах гібридної війни наша держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод, що є стратегічно важливим завданням держави для забезпечення інтересів національної безпеки.

Тому інформаційна безпека набуває особливого значення в сучасних умовах глобалізації та міжнародної інтеграції в період режиму воєнного стану в Україні.

Держави з великим потенціалом в інформаційному середовищі можуть впливати на країни, інформаційний простір яких є незахищеним.

За останні три роки в Україні реалізовано більше заходів щодо забезпечення інформаційної безпеки в інформаційній сфері, ніж за весь попередній період незалежності.

Протидія інформаційним операціям переконливо показує, що хоча вони в основному плануються та організовуються з-за кордону, вони залежать від оперативного положення та можливостей, які є всередині країни, в якій такі операції проводяться.

Загалом російські інформаційні операції характеризуються тим, що вони плануються та здійснюються в рамках єдиного оперативного плану та спільного стратегічного впливу, відрізняючись лише формою та способом реалізації та вибором цільових груп.

За цих обставин не можна недооцінювати роль і значення Служби безпеки України в забезпеченні інформаційної безпеки в Україні.

Логічно, що в положеннях стратегії інформаційної безпеки важлива роль відводиться діяльності національних спецслужб, які в межах своїх повноважень відповідатимуть спеціальним методам національних та іноземних ЗМІ та уряду.

Проводити моніторинг з використанням відповідних методів. Інтернет для виявлення реальних і потенційних загроз національній безпеці в окремих інформаційних сферах. Організовувати та вживати заходів протидії проведенню спеціальних розвідувальних операцій проти України, зокрема російської федерації, спрямованих на підрив конституційного ладу та порушення суверенітету та територіальної цілісності України.

Свідоме маніпулювання громадською думкою за допомогою інформаційних технологій та психологічного впливу є одним із найнебезпечніших проявів гібридної війни, яку держава-агресор веде проти України.

Інформаційна безпека – це стійка, стаціонарна характеристика типової системи управління державою, яка підтримує критичні компоненти навіть під впливом внутрішніх і зовнішніх загроз.

Інформаційна безпека відповідає за захист громадян і національних інтересів в інформаційному полі від різних загроз, реальних і гіпотетичних.

Концепція інформаційної безпеки України проявляється в її стратегії виживання як суверенної та стабільної держави, а також у розробці та реалізації цілеспрямованої, системної та виваженої політики захисту національних інтересів від внутрішніх та зовнішніх інформаційних загроз.

Важливі та актуальні закони, які узагальнюють нагальні та поточні питання забезпечення безпеки у вітчизняному інформаційному просторі, є Стратегія інформаційної безпеки держави, яка розрахована на наступні п'ять років (2022 – 2025 рр.) затверджена Указом Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»[1] та відповідно до статті 107 Конституції України [2], статті 13 Закону України «Про Національну безпеку України»[3].

У положеннях вказаної Стратегії концептуально розкриваються такі важливі для нашої держави аспекти, як глобальні та національні загрози й виклики для вітчизняної інформаційної безпеки; завдання та напрями реалізації базових положень Стратегії; засади стратегічного планування у цій сфері; методологія досягнення результативності виконання її базових положень; механізми успішної реалізації її положень у практичну площину в контексті розбудови засад державної інформаційної політики.

Імперативом національного стратегічного планування залишається раціональний розподіл нацією потенційних можливостей і наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, інженерних, технологічних), щоб нація гарантувала безпеку та стабільні соціально-економічні умови, цифровий розвиток громадянського суспільства.

Досягнення цієї мети потребує достатньо витонченої культури керівництва державними установами та використання методів системного аналізу та прогнозування забезпечення інформаційної безпеки.

Стратегічне планування у сфері забезпечення інформаційної безпеки може значно підвищити ефективність та якість державного управління у цій сфері.

Стратегічне планування має розглядатися всіма національними органами влади та управління як універсальний інструмент, завдяки якому можлива реалізація поточних загальнодержавних завдань у сфері забезпечення інформаційної безпеки, у тому числі з використанням механізмів державно-приватного партнерства.

У сьогоднішній ситуації суспільство в цілому, особливо державно-громадський сектор ІТ-сфери, відчуває на собі вплив триваючої агресії російської федерації, яка має гібридний характер та проникає в інформаційний простір та завдає значних збитків.

російська федерація використовує сучасні технології, такі як соціальні мережі та системи мікроблогів, для маніпулювання суспільною свідомістю, розпалювання соціальної напруги та поширення забороненої законом інформації.

В сучасних реаліях гібридна війна стає інтенсивнішою і набуває нових форм. Тому спецслужбам необхідно враховувати інноваційні гібридні загрози з боку російської федерації та надати їм додаткові механізми протидії таким загрозам.

З метою недопущення та стримування російською федерацією такого сценарію «керованого хаосу» вітчизняні спецпідрозділи насамперед спрямовані на недопущення такої підривної діяльності, що завдає шкоди державі, необхідно посилити спроможність країни проводити контррозвідувальні операції [5].

Основними завданнями, які мають залишатися в компетенції Служби безпеки

України, є: виявлення представників екстремістської спрямованості у вітчизняних засобах масової інформації та недопущення їх використання іноземними організаціями та їх філіями для підриву безпеки України, здійснення заходів, спрямованих на запобігання та протидії таким загрозам на території України, система додаткових заходів, спрямованих на недопущення розповсюдження в засобах масової інформації та мережі Інтернет контенту, що порушує національний суверенітет та територіальну цілісність України, розпалює міжнаціональні та релігійні конфлікти, пропагандує війну тощо.

Тому очікуваними результатами реалізації Стратегії є: захищений інформаційний простір України; ефективне функціонування системи стратегічних комунікацій; здійснення ефективної протидії поширенню незаконного контенту; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіакультури та медіаграмотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя; забезпечення захисту прав журналістів; формування української громадянської ідентичності [1].

Отже, реальна реалізація цієї стратегії посилить здатність Української нації забезпечувати власну інформаційну безпеку та захист свого інформаційного простору в умовах режиму воєнного стану в Україні, де росія є основною загрозою безпеці України.

1. Стратегія інформаційної безпеки: Указ Президента України від 28.12.2021р.№685/2021.URL :https://zakon.rada.gov.ua/laws/show/685/2021# Text

2. Конституція України від 28.06.1996 р. URL https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

3. Про Національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text

4. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1(24)/2018. С. 89-103.

5. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 411 с.

УДК 35.078.7/759.6
DOI: 10.31733/15-03-2024/2/326-328

Олександра
НЕСТЕРЦОВА-СОБАКАРЬ
доцент кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ УКРАЇНИ

Зростання інформаційної інфраструктури, що виникає у суспільних відносинах, призводить до того, що національна безпека має суттєву залежність від забезпечення інформаційної стійкості та надійності основних її компонентів. Ця проблема має системотворче значення для розвитку держави у всіх сферах життєдіяльності суспільства, так і щодо забезпечення безпеки країни в цілому.

Основною проблемою є забезпечення інформаційної безпеки, яка сприяє захищеності інформації від несанкціонованого доступу, використання, розкриття, зміни, знищення, а також від випадкового чи навмисного впливу, що може призвести до втрати, крадіжки, пошкодження, модифікації чи недоступності інформації. Інформаційна безпека має велике значення для забезпечення захисту державних таємниць, а також інформаційних систем та ресурсів державних органів; захисту конфіденційної інформації, комерційної таємниці, а також інформаційних систем та бізнес-ресурсів, захисту персональних даних, доступності інформації та її незмінності; контролю за доступом до інформації та її