# СТРАТЕГІЧНІ ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

# STRATEGIC PRIORITIES OF THE ENSURING THE INFORMATION SECURITY IN CONDITIONS OF WAR

УДК 351:342.7
DOI https://doi.org/10.32782/pma2663-5240-2024.39.39

**Руденко О.М.,**
доктор наук з державного управління, професор,
завідувач кафедри менеджменту та адміністрування,
Національний університет «Чернігівська політехніка»
ORCID ID: 0000-0002-2807-1957

**Захаров М.В.,**
здобувач ступеня доктора філософії,
Національний університет «Чернігівська політехніка»
ORCID ID: 0009-0004-3457-3760

*У статті визначено стратегічні пріоритети забезпечення інформаційної безпеки в умовах війни. Показано, що проект Концепції інформаційної безпеки України містить більш адаптовані до умов війни стратегічні пріоритети та цілі порівняно з діючою Стратегією інформаційної безпеки України. Це спонукає переглянути Стратегію, скорегувавши стратегічні цілі, які вона встановлює, віддавши пріоритет саме тим стартегічним цілям у сфері забезпечення інформаційної безпеки держави, які є найбільш актуальними під час війни. необхідність формування сучасного підходу до забезпечення інформаційної безпеки держави, який би враховува особливості ведення боротьби в умовах гібрідних війн та збройної боротьби. Аргументовано, що поряд з очевидною необхідністю і раціональністю визначених державною інформаційною політикою та стратегією інформаційної безпеки держави стратегічних цілей і завдань, в умовах війни не всі вони є актуальними, доречними та своєчасними. Головного пріоритету в умовах війни набувають ті стратегічні цілі та завдання у сфері забезпечення інформаційної безпеки, які спрямовано на забезпечення воєнної безпеки в цілому і які сприяють створенню ситуації, в якій противник обмежується у здатнсті маніпулювати суспільною та індивідуальною свідомістю, колективним мисленням, посилюючи резистентну здатність системи національної безпеки в цілому протистояти викликам і загрозам воєнного часу. Важливим аспектом у цьому контексті є здатніст протидіяти інформаційно-спихологічним операціям противника, що потребує проведення комплексу заходів (у тому числі, за допомогою технічних засобів) у звичайному, віратуальному та кіберпросторі, що здійснюються у рамках і на підтримку вирішення військових завдань, досягнення стратегічних і тактичних цілей на театрі воєнних дій. Підкреслюється, що інші стратегічні цілі та завдання у сфері забезпечення інформаційної безпеки також не втрачають свого значення, залишаючись основним елементом реалізації державної інформаційної політики та забезпечуюючи державі адекватну репрезентативність в системі колективної безпеки. Їх пріоритетність в умовах війни має мінімізуватись такими необхідними заходами, як введення і досягнення повного контролю (у тому числі за допомогою технічних засобів) над всіма засобамиіндивідуальної та суспільної комунікації, встановлення і забезпечення цензури та тимчасових обмежень свободи слова поряд з посиленням діяльності всіх складових сил безпеки у сфері забезпечення і дотримання всіх принципів законності.*

**Ключові слова:** *війна, забезпечення інформаційної безпеки, інформаційна безпека, інформаційна безпека держави, інформаційна війна, національна безпека, стратегія інформаційної безпеки.*

*The article deals with defines the strategic priorities of ensuring information security in wartime conditions. It is shown that the draft Information Security Concept of Ukraine contains strategic priorities and goals more adapted to war conditions compared to the current Information Security Strategy of Ukraine. This prompts us to revise the Strategy, adjusting the strategic goals it sets, giving priority to those strategic goals in the field of ensuring the information security of the state, which are most relevant during the war. the need to develop a modern approach to ensuring the information security of the state, which would take into account the peculiarities of fighting in the conditions of hybrid wars and armed struggle. It is argued that along with the obvious necessity and rationality of the strategic goals and objectives defined by the state information policy and information security strategy of the state, not all of them are relevant, relevant and timely in the conditions of war. Those strategic goals and tasks in the field of ensuring information security that are aimed at ensuring military security as a whole and that contribute to creating a situation in which the enemy is limited in the ability to manipulate public and individual consciousness, collective thinking, strengthening the system's resistant capacity, acquire the main priority in the conditions of war national security as a whole to face the challenges and threats of wartime. An important aspect in this context is the ability to counteract the information and psychological operations of the enemy, which requires the implementation of a set of measures (including, with the help of technical means) in ordinary, virtual and cyberspace, carried out within the framework of and in support of solving military tasks, achieving strategic and tactical objectives in the theater of war. It is emphasized that other strategic goals and objectives in the field of ensuring information security also do not lose their importance, remaining the main element of the implementation of the state information policy and providing the state with adequate representativeness in the system of collective security. Their priority in the conditions of war should be minimized by such necessary measures as the introduction and achievement of full control (including with the help of technical means) over all means of individual and public communication, the establishment and provision of censorship and temporary restrictions on freedom of speech, along with the strengthening of the activities of all components of the security forces in the field of ensuring and observing all principles of legality.*

**Key words:** *ensuring the information security, information security, information security of state, information war, national security, strategy of information security, war.*

**Постановка проблеми.** Інформаційні заходи стали невід'ємною частиною діяльності всіх складових сил безпеки в оборони держави у процесі забезпечення інформаційної безпеки та однією з основних складових ведення інформаційних війн, спрямованих на досягнення перемоги не лише на полі бою, а також в інформаційному просторі, адже сучасні війни ведуться значною мірою в інформаційному просторі, що дозволяє кожній зі сторон протиборства створити умови для отримання еперваги над противником з найменьшими втратами техніки та живої сили. Ідеологічна перемога над противником є запорукою отримання повного контролю над захопленими противником територіями, отримання цих територій інколи навіть без проведення військових операцій та бойових дій. Це привертає особливу увагу до забезпечення інформаційної безпеки держави в умовах війни, адже далеко не всі держави мають розвинену систему її забезпечення та підтримки, яка б чітко визначала особливості іфнормаційної боротьби в умовах миру та війни. Безумовно, Україна має значні досягнення у цій сфері, але державна інформаційна політика, як і стратегічні пріоритети у сфері забезпечення інформаційної безпеки держави залишаються малоадаптованими до умов ведення війни, орієнтуючись переважно на пріоритети зовнішньої політики мирного часу. Це створює загрозливу ситуацію, пов'язану з величезною активністю противника у сфері ведення інформаційної боротьби, що потребує перегляду основних принципів, пріоритетів та стратегічних орієнтирів забезпечення інформаційної безпеки України.

**Аналіз наукових публікацій**. Проблемні питання забезпечення інформаційної безпеки досліджували В. Довгань [4], Т. Ткачук [11], О. Солодка [9]. Н. Тарасенко [10], С. Гордієнко [3], А. Турчак [12] звертали увагу на аналіз положень Доктрини інформаційної безпеки України. Загальні принципи забезпечення інформаційної безпеки держави в системі національної безпеки, у тому числі в аспекті протидії загрозам, що виникають в умовах війни та воєнного стану, досліджували Л. Браілко [8], Д, Вітер [1; 16; 17], М. Гаврильців [2], І. Залєвська [5], В. Новицький [6], О. Руденко [1], Д. Смотрич [8], Г. Удренас [5], О. Цевельов [16; 17] та інші дослідники. Водночас, недостатньо уваги приділено питанням державного регулювання і забезпечення інформаційної безпеки держави в умовах військового стану та війни в контексті впливу на систему національної безпеки в цілому загроз, що притаманні гібридним війнам, у контексті чого мають бути чітко визначені стратегічні пріоритети забезпечення інформаційної безпеки.

**Метою статті** є визначення стратегічних пріоритетів забезпечення інформаційної безпеки в умовах війни.

**Виклад основного матеріалу.** Неможливо переоцінити важливість забезпечення інформаційної безпеки держави в умовах війни, яка, маючи характер гібридної, активно перетворюється на інформаційну війну, без перемоги в якій неможливо досягнути перемоги на полі бою. Агрессор наразі використовує широкий спектр засобів ведення інформаційних війн та проведення інформаційно-психологічних операцій. Так, «для проведення інформаційно-психологічних операцій на полі бою залучено спеціальні підрозділи збройних сил РФ. До комплекту російських частин інформаційно-психологічного впливу на сході України увійшли:

– групи спеціальних журналістів (8-10 окремих груп) – які працюють безпосередньо на російські інформаційні канали. До їх складу входять 3-4 особи – журналіст, оператор, водій може бути охоронець. Групи готувалися до умов війни напередодні та мають чіткі інструкції про те, як висвітлювати події. Вони добре оснащені, мають перепустки по всій території Донбасу, контрольованого збройними силами противника;

– оперативні групи психологічних операцій (4 групи ПсО) – є мобільні підрозділи від загону ПсО, дислокованого неподалік Ростова-на-Дону. Їхній склад 2-4 особи.

На території окупованого Донбасу вони виконують завдання:

– усній пропаганді, у тому числі й роботі з місцевим населенням;

– поширення пропагандистської літератури та іншої необхідної інформації;

– створення пропагандистських груп у населених пунктах, що складаються з місцевих активістів, їх організації та координації дій;

– надання сприяння роботі російських журналістів;

– збір інформації та визначення найбільш гострих проблем у населення для використання цього надалі, як інформаційного приводу;

– моніторинг поточного морально-психологічного стану місцевого населення» [16, с. 73].

Крім цього, активний вплив на суспільну та індивідуальну свідомість громадян здійснює агентурна мережа противника на території України, зокрема, «агенти диверсійної психологічної роботи в інших областях України – фахівці від Головного розвідувального управління генерального штабу збройних сил або

Федеральної служби безпеки РФ, які виконують завдання з:

– створення диверсійно-пропагандистських груп в інших областях України серед місцевого авторитетного населення;

– навчання місцевих груп проведенню підривних пропагандистських акцій;

– забезпечення груп необхідним матеріально-технічним майном;

– безпосередньому проведенню мітингів, акцій протесту та поширенню пропагандистських матеріалів» [16, с. 74].

Така увага противника до ведення інформаційних війн, проведення інформаційно-психологічних операцій потребує від України вироблення чіткої стратегії інформаційної безпеки, визначення основних пріоритетів та завдань реалізації основних принципів забезпечення інформаційної безпеки в системі національної безпеки держави під час ведення війни.

До початку війни у 2017 році з метою забезпечення інформаційної безпеки в Україні було затверджено «Доктрину інформаційної безпеки України» [13]. Пізніше, у 2021 році, на розвиток Доктрини інформаційної безпеки України, було затверджено Стратегію інформаційної безпеки України (далі – Стратегія), яка визначала сім основних стратегічних цілей у сфері інформаційної безпеки України [14]:

1. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету та територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, проведення терористичних актів, посягання на права та свободи людини.

2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.

3. Підвищення рівня медіакультури та медіаграмотності суспільства.

4. Забезпечення інформаційних прав особи, захисту прав журналістів.

5. Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, до загальноукраїнського інформаційного простору.

6. Створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної інформаційної взаємодії між органами державної влади, органами місцевого самоврядування та суспільством з питань кризових ситуацій. Зміцнення позитивного іміджу України.

7. Розвиток інформаційного суспільства та підвищення рівня культури діалогу.

Проте, більшість визначних у Стратегії стратегічних цілей не враховували особливості забезпечення інформаційної безпеки суспільства, держави і особистості в умовах війни. Складні умови, пов'язані з веденням бойових дій, протистояння агресії, втратою значних територій держави, які виявились тимчасово окупованими, вимагають перегляду стратегічних цілей, визначених у Стратегії. Тільки дві цілі Стратегії мають відношення до функціонування системи забезпечення інформаційної безпеки в умовах військового часу та війни, це – протидія дезінформації та інформаційним операціям, насамперед держави-агресора (Стратегічна ціль 1), та частково – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України (Стратегічна ціль 5).

Після початку повномасштабної війни 18 березня 2022 року було прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки» [15]. Проте, конкретних стратегічних пріоритетів та шляхів забезпечення інформаційної безпеки, а також формування і реалізації інформаційної політики в умовах військового стану та війни рішення РНБО не запропонувало.

План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затверджений Розпорядженням Кабінету Міністрів України у 2023 році, розширив перелік стратегічних завдань, які необхідно вирішити на виконання стратегічних цілей, визначених Стратегією [7]. Цей План містить більш чіткий перелік стратегічних завдань, які безпосередньо пов'язані із забезпеченням функціонування суспільства і держави в умовах військовго стану та війни. Зокрема, на забезпечення Стратегічної цілі 1 передбачено виконання, серед інших, таких завдань:

– створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози;

– розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі;

– підготовка та проведення складовими сил оборони інформаційно-психологічних

операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України.

Їх важливість зумовлена тим, що «повномасштабна агресія РФ проти України не обходиться без інформаційно-психологічних атак з боку російських збройних сил та спеціальних служб, які їх підтримують, а центри інформаційно-психологічних операцій (ІПСО) – це саме той військовий елемент, який може забезпечувати ефективне протистояння противнику не тільки в інформаційній боротьбі» [1].

На забезпечення Стратегічної цілі 5 передбачено, серед інших, виконання наступних завдань:

– створення умов для задоволення потреб населення тимчасово окупованих територій в об'єктивній та достовірній інформації шляхом забезпечення стабільного функціонування національного телебачення та радіомовлення на тимчасово окупованих територіях, на територіях, які розташовані на лінії зіткнення;

– спростування дезінформації, яка поширюється у суспільстві.

Важливість цих завдань зумовлена можливістю «зменшити втрати ЗС та збільшити потік інформації про порушення ворогом умов ведення війни через інформаційно-комунікативну систему проводиться компанія «віктимізації за довіреністю» (формування макровіктимного мислення) шляхом поширенням фейків і посиленою пропагандистською кампанією всередині країн ЄС та США, спрямованою на протидію РФ. У даному випадку вибірковість у підборі інформації та атаках на свідомість людей – обов'язковий механізм віктимізації» [1].

Водночас, реалізація визначених Стратегією стратегічних цілей та завдань потребує доопрацювання відповідно сучасному стану забезпечення інформаційної безпеки (перш за все, в умовах військовго стану та війни) Концепції інформаційної безпеки України, яка має забезпечити протидію комплексу загроз інформаційній безпеці України, що передбачає наступне [Концепція інформаційної безпеки України (проект) // https://www.osce.org/files/f/documents/0/2/175056.pdf.]:

1. Державна політика у сфері інформаційної безпеки здійснюється з метою недопущення перешкоджання реалізації життєво важливих інтересів і потреб громадянина, суспільства і держави зовнішніми і внутрішніми загрозами національній безпеці в інформаційній сфері.

2. Загрозами національній безпеці України в інформаційній сфері є: загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації; загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору.

3. Загрози комунікативного характеру, що включають:

а) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет з метою зміни психічного та емоційного стану людини, її психологічних і фізіологічних характерист; здійснення керованого впливу на свободу вибору; поширення закликів до сепаратизму, повалення конституційного ладу чи порушення територіальної цілісності держави;

б) інформаційний вплив на населення України, у тому числі на особовий склад військових формувань, мобілізаційний резерв, з метою послаблення їх готовності до оборони держави;

в) поширення суб'єктами інформаційної діяльності інформації, яка дискредитує органм державної влади, дестабілізує суспільно-політичну ситуацію тощо.

4. Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору включають:

а) використання іноземними державами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;

б) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, незалежно від форми власності, з метою: вчинення диверсій чи терористичних актів; здійснення підтримки, супроводження чи активізації злочинної, екстремістської чи терористичної діяльності; здійснення з їх допомогою деструктивного інформаційного впливу; перехоплення інформації в телекомунікаційних мережах; створення радіоелектронних перешкод чи блокування інформаційних систем, засобів зв'язку та управління, реалізація програмно-математичних засобів, що порушують функціонування інформацій-

них систем; включення у програмно-технічні засоби прихованих шкідливих функцій тощо.

Як можна побачити, запропонований проект Концепції інформаційної безпеки України містить більш адаптовані до умов війни стратегічні пріоритети та цілі порівняно з діючою Стратегією. Це спонукає переглянути Стратегію, зкорегувавши стратегічні цілі, які вона встановлює, віддавши пріоритет саме тим стартегічним цілям у сфері забезпечення інформаційної безпеки держави, які є найбільш актуальними під час війни.

**Висновки.** Поряд з очевидною необхідністю і раціональністю визначених державною інформаційною політикою та стратегією інформаційної безпеки держави стратегічних цілей і завдань, в умовах війни не всі вони є актуальними, доречними та своєчасними. Головного пріоритету в умовах війни набувають ті стратегічні цілі та завдання у сфері забезпечення інформаційної безпеки, які спрямовано на забезпечення воєнної безпеки в цілому і які сприяють створенню ситуації, в якій противник обмежується у здатнсті маніпулювати суспільною та індивідуальною свідомістю, колективним мисленням, посилюючи резистентну здатність системи національної безпеки в цілому протистояти викликам і загрозам воєнного часу. Важливим аспектом у цьому контексті є здатніст протидіяти інформаційно-спихологічним операціям противника, що потребує проведення комплексу заходів (у тому числі, за допомогою технічних засобів) у звичайному, віратуальному та кіберпросторі, що здійснюються у рамках і на підтримку вирішення військових завдань, досягнення стратегічних і тактичних цілей на театрі воєнних дій. Інші стратегічні цілі та завдання у сфері забезпечення інформаційної безпеки також не втрачають свого значення, залишаючись основним елементом реалізації державної інформаційної політики та забезпечуючи державі адекватну репрезентативність в системі колективної безпеки. Хоча їх пріоритетність в умовах війни має мінімізуватись такими необхідними заходами, як введення і досягнення повного контролю (у тому числі за допомогою технічних засобів) над всіами засобамиіндивідуальної та суспільної комунікації, встановлення і забезпечення цензури та тимчасових обмежень свободи слова поряд з посиленням діяльності всіх складових сил безпеки у сфері забезпечення і дотримання всіх принципів законності.

**ЛІТЕРАТУРА:**

1. Вітер Д., Руденко О. Інформаційно-комунікативна складова мережевої протидії загрозам національній безпеці у воєнній сфері. *Society and Security*. № 1(2), 2024. С. 119-123.

2. Гаврильців М. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200-203.

3. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. *Юридичний вісник*. 2019. № 3. С. 22-28.

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

5. Залєвська І., Удренас Г. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*, 2022. № 1-2. С. 20-26.

6. Новицький В. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і Право*. 2022. № 1(40). С. 111-118.

7. Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року». URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text.

8. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. 2023. Вип. 77. Ч. 2. С. 121-127

9. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. Інформація і право. № 3(15)/2015. С. 36-42.

10. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Резонанс*. 2017. № 18. С. 3-14.

11. Ткачук Т. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монограф. К.: ТОВ “Видавничий дім “АртЕк”. 2018. 411 с.

12. Турчак А. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід*. 2019. № 11. С. 123-127.

13. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://zakon.rada.gov.ua/go/47/2017.

14. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7.

15. Указ Президента України від 19 березня 2022 року № 152/2022 «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://zakon.rada.gov.ua/go/152/2022.

16. Цевельов О., Вітер Д. Російсько-Українська війна: холодна весна 2022: моногр. К.: НУОУ. 2022. 104 с.

17. Цевельов О., Вітер Д. Російсько-українська війна: причини, хід ведення та наслідки (огляд подій та хід ведення бойових дій 2022-2023 років): монограф. К.: Талком. 2024. 372 с.