УДК 351:342.7
DOI https://doi.org/10.32782/TNU-2663-6468/2024.1/44

Захаров М.В.
Національний університет «Чернігівська політехніка»
ORCID ID: 0009-0004-3457-3760

КОНЦЕПТУАЛІЗАЦІЯ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВІЙНИ

У статті здійснено аналіз підходів до визначення змісту та сутності інформаційної безпеки держави. Обгрунтувано необхідність формування сучасного підходу до забезпечення інформаційної безпеки держави, який би враховува особливості ведення боротьби в умовах гібрідних війн та збройної боротьби. Аргументовано, що принципи, покладені в основу проекта Концепції інформаційної безпеки України не повінстю відповідають тим завданням, які виникають перед державою та суспільством в умовах війни. Створюючи загальні умови та проваджуючи загальні принципи забезпечення інформаційних прав і свобод, ті чи інші регулятиві інформаційного простору, положення Концепції інформаційної безпеки України сприяють формуванню та розвитку інформаційного суспільства, залишаючи поза увагою той факт, що таке суспільство в умовах ведення агресивних війн стає першим об'єктом впливу, забезпечуючи противнику сприятливі умови гібридного впливу на суспільство, державу і особистість, тобто акутине та ефективне ведення інформаційних війн. У цьому аспекті обгрунтовано, що інформаційна безпека держави має грунтуватись на концептуальному положенні системного підходу до дослідження проблем національної безпеки, на основі якого інформаційна безпека держави у своєму змісті набуває визначальних характеристик ступеня захищеності і стійкості основних сфер життєдіяльності держави і суспільства, що забезпечують резистентну здатність системи протистояти небезпечним (дестабілізаційним, деструктивним) чинникам інформаційного середовища, інформаційним впливам на всіх етепах розповсюдження та обміну інформації.

Ключові слова: *війна, інформаційна безпека, інформаційна безпека держави, інформаційна війна, концептуалізація, національна безпека, підхід.*

Постановка проблеми. Війни нового покоління вимагають від держав формування особливого ставлення до інформаційної безпеки. Гібридний характер сучасних війн висуває в якості однієї з важливих вимог ведення протистояння між державами набуття спроможності входити й вести активні дії в інформаційному просторі, що стає сьогодні одним з вирішальних факторів протистояння військовій агресії. Це стосується всіх складових системи національної безпеки. Але однією з важливих проблем на даний час залишається забезпечення інформаційної безпеки держави, оскільки сфера інформаційної безпеки характеризується стрімким розвитком таких сутністних її характеристик, як віртуальність, внаслідок чого боротьба переноситься у сферу кіберпростору, який за наслідками впливу на свідомість особистості (як базового об'єкту інформаційного впливу) виявляється більш потужним, ніж навіть безпосередні бойові дії із застосуванням летальної зброї. Як підкреслюють дослідники, повномасштабна агресія проти України не обходиться без інформаційно-психологічних атак з боку російських збройних сил та спеціальних служб, які їх підтримує, а центри ІПСО – це саме той військовий елемент, який може цьому протистояти. З боку України також здійснюється потужна інформаційна боротьба, що має свою користь у майбутньої перемоги. Сьогоднішня дійсність України наочно підтвердила, що буквально всі дипломатичні, економічні, військові, політичні та інші кроки держави здійснюються у тісному інформаційному супроводі. Сила сучасної держави залежить не лише від її економічного та політичного потенціалу, а й від власної системи інформаційної безпеки [9]. Останнє актуалізує вирішення питання забезпечення інформаційної безпеки держави в умовах воєнного стану та війни.

Аналіз досліджень і публікацій. Проблематику інформаційної безпеки як складової національної безпеки, різноманітні аспекти публічного управління, формування та реалізації державної політики у сфері забезпечення інформаційної безпеки держави долсіджували В. Абрамов, О. Бара-

новський, І. Бінько, З. Варналій, Д. Вітер, О. Власюк, А. Гальчинський, В. Горбулін, Н. Грицяк, А. Качинський, В. Мунтіян, О. Руденко, Г. Ситник та інші вітчизняні дослідники. Водночас, питання підходу до визначення змісту та сутності поняття інформаційної безпеки, його трансформації в умовах воєнного стану та сучасної війни залишаються малодослідженими.

Метою статті є концептуалізація підходів до інформаційної безпеки в умовах воєнного стану та війни.

Виклад основного матеріалу. Питання забезпечення інформаційної безпеки держави з початком повномасштабної війни проти України посіло одне з провідних місць. Як підкреслюють дослідники, з початку війни в Україні «найвідчутніший результат мала зміна інформаційної політики держави у сфері оборони. Якщо в перші дні спостерігався спокійний, більш оборонний підхід Міністерства оборони України, то сьогодні інформаційна війна стала потужною ніж самі бойові дії», чому сприяло створення центру інформаційної спеціальної пропаганди та кіберзахисту при Міністерстві оборони України у взаємодії з спеціальним підрозділом Служби безпеки України, внаслідок чого наразі «інформаційне забезпечення дій українських військ здійснюється на дуже високому рівні» [9, с. 32–33]. Водночас важливо розуміти, що «в умовах сьогодення основний акцент в сучасній війні, що стосується проведення силових операцій, змінюється в сторону досягнення цілей боротьби несиловими способами так званими «гібридними», а саме проведенням інформаційних, психологічних та цивільних (у тому числі, цивільно-військових) операції» [11]. Це у сукупності привертає увагу до сталих підходів до вирішення проблем забезпечення національної безпеки в цілому та інформаційної безпеки держави зокрема, які є основою розуміння змісту та сутності інформаційної безпеки.

Так, згідно діючої нормативно-правової бази інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем, як правило, розуміється конкретна сфера діяльності суб'єктів соціального управління, яка пов'язана зі створенням, перетворенням і споживанням інформації. Відповідно, інформаційне середовище поділяється на [3; 4; 7]: створення і розповсюдження вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації; створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення; створення і застосування засобів і механізмів інформаційної безпеки.

Наведений вище умовний поділ інформаційного середовища свідчить про переважання у вирішенні проблем інформаційної безпеки утилітарного підходу, який поєднує в собі традиційний інформаційний або кібернетичний (фактичне ототожнення поняття інформаційної безпеки із захистом інформації) та політологічний (вивищення компенсаторної функції та принципу гомогенності) підходи до вирішення проблем національної безпеки в цілому та інформаційної безпеки держави зокрема.

Такий підхід має наслідком і особливості визначення принципів забезпечення інформаційної безпеки, серед яких дослідники виділяють наступні специфічні, тобто такі, що стосуються виключно сфери інформаційної безпеки, принципи [3; 7; 8]: превентивний характер проведення її заходів стосовно заходів інших видів безпеки; адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

За змістом принцип превентивності, який «зумовлений властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію», фактично співпадає з підходом до аналізу операцій, поширеним в операційному управлінні та менеджменті. Як зазначають дослідники [5, с. 34], «все починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. Оскільки це справедливо по відношенню до будь-якого виду діяльності, то можна стверджувати, що цей принцип є загальним, і його дія розповсюджується на всі сфери безпеки особистості, суспільства та держави» [5, с. 34]. Втім, такий підхід справедливий поза межами ведення інформаційної боротьби, гарантуючи можливість створення певних базових умов забезпечення інформаційної безпеки у мирний час.

У свою чергу, адекватна інформованість об'єктів безпеки, як специфічний принципів забезпечення інформаційної безпеки, означає, що всі суб'єкти сфери безпеки особистості, суспільства та держави «мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі» [5, с. 34].

В якості результату застосування наведених приниципів та підходи до забезпечення інформаційної безпеки формується концепт державної системи забезпечення інформаційної безпеки, який являє собою «організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є: а) виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави; б) здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення; в) створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки» [3]. Проте, якщо звернути увагу на основні завдання системи захисту інформації, яку пропонують дослідники, то можна побачити, що така система є суттєво редукованою орієнтацією на майже виключно внутрішні процеси обміну інформацією та намагання регулювати ці процеси в самій системі. Зокрема, на думку В. Горника та С. Кравченко, основними завданнями системи захисту інформації можна вважати наступні [3]:

– організація особливого діловодства та контролю за секретними документами;

– виявлення, попередження та присікання каналів витікання інформації;

– створення посадових інструкцій, а також положень, пам'яток, методичних вказівок для роботи з відомостями, що складають комерційну таємницю;

– захист інформації під час використання комп'ютерної техніки та інших технічних засобів обробки та передавання даних;

– виявлення необхідності, обґрунтування та організація встановлення необхідних технічних засобів забезпечення збереження інформації;

– захист у судових та інших державних органах інтересів підприємства щодо комерційної таємниці;

– розроблення нормативної документації щодо комерційної таємниці на підприємстві;

– навчання правилам інформаційної безпеки працівників.

Вказані завдання лише частково створюють умови для протидії негативній інформації, зменшуюючи обсяги її потрапляння в систему, що обмежує резистентну здатність системи під час ведення інформаційної боротьби, а також уникненню або мінімізації впливу негативних чинників зовнішнього середовища. Це не в останню чергу обмувлено особливостями інформації як такої, яка завжди поєднує в собі позитивний і негативний потенціал, здатний дестабілізувати суб'єкт або систему. Так, аналізуючи особливості застосування Сил спеціальних операцій у рамках інформаційно-комунікативна складової мережевої протидії загрозам національній безпеці у воєнній сфері під час війни, дослідники зазначають, що «стратегія стримування здебільшого інтегрована в Воєнну стратегію України, яка містить у собі всі елементи національної влади: дипломатичну, інформаційну, військову та економічну, спрямована на організацію всебічного національного опору агресору. І якщо військовий компонент цієї стратегії передбачає операції стримування на окупованих територіях, які мають працювати разом з веденням основних бойових дій щодо звільнення окупованої території, то інформаційний компонент поки ще потребує активного розвитку та урахування в якості одного з визначальних факторів у сучасних конфліктах» [1, с. 123]. Відповідно, коли йдеться про ведення інформаційної боротьби та забезпечення інформаційної безпеки в умовах воєнного стану або війни до основних заходів та завданьсистеми інформаційного захисту в цілому необхідно включати інформаційне забезпечення інформаційної безпеки, що передбачає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами управління, силами та засобами системи інформаційної безпеки (розвідувальна, контррозвідувальна оперативно-розшукова і оперативно-інформаційна діяльність).

Доцільно звернути увагу на підхід, за яким «дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмета, який виражається у стійкій єдності всіх різноманітних і суперечливих формах буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Отже, можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональ-

них або інших національно-державних структур у межах міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають це утворення. У ролі останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління» [5]. На основі застосування наведеного підходу зазвичай формується концепція інформаційної безпеки держави, яка являє собою систематизовану сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. Концепція інформаційної безпеки держави містить: системну класифікацію дестабілізуючих факторів і інформаційних загроз безпеці особистості, суспільства і держави; обґрунтовує основні положення з організації забезпечення інформаційної безпеки держави; пропозиції щодо способів і форм забезпечення інформаційної безпеки [4, с. 24–25].

Концептуалізація основних принципів та підходів до забезпечення інформаційної безпеки дає можливість визначити напрями державної політики у сфері інформаційної безпеки, що є невід'ємною складовою всієї системи забезпечення інформаційної безпеки, набуваючи особливого значення під час війн та суспільних конфліктів. На сьогодні проектом Концепції інформаційної безпеки України, розробленим у відповідності до методичних рекомендацій ОБСЄ, визначено наступні основні напрями державної політики у сфері забезпечення інформаційної безпеки [6]:

– забезпечення балансу між неухильним дотриманням конституційних прав і свобод людини в інформаційній сфері, зокрема свободи слова, та реалізацією державних функцій щодо своєчасного виявлення, запобігання, припинення та нейтралізації загроз інформаційній безпеці людини і громадянина, суспільства і держави;

– розвиток нормативно-правової бази для регулювання процесів розвитку інформаційного простору і його захисту від зовнішніх загроз та її гармонізація з нормами міжнародного права, вимогами міжнародного співробітництва, нормами і стандартами Європейського Союзу;

– розробка та реалізація ефективної державної інформаційної політики з метою розвитку національного інформаційного простору та гармонізації системи управління і координації між суб'єктами, які реалізують державну інформаційну політику та державну політику в сфері інформаційної безпеки;

– налагодження співпраці держави з громадським та приватним секторами, а також сприяння міжнародному співробітництву з метою реалізації державної інформаційної політики та забезпечення інформаційної безпеки, а також створення якісного національного інформаційного продукту;

– всебічне сприяння, державна підтримка та пріоритетність створення і розповсюдження національного інформаційного продукту, в тому числі за межі України;

– використання українського національного інформаційного продукту для поширення в міжнародному інформаційному середовищі загальнолюдських цінностей та інформаційного розвитку людства, зокрема обмін із закордонними партнерами України баченням, підходами та механізмами протистояння новітнім викликам, спрямованим на демократичні цінності та свободу слова в інформаційному просторі, що були інспіровані деструктивною політикою інших держав.

Проте, принципи, покладені в основу проекта Концепції інформаційної безпеки України також не відповідають тим завданням, які виникають перед державою та суспільством в умовах війни. Створюючи загальні умови та проваджуючи загальні принципи забезпечення інформаційних прав і свобод, ті чи інші регулятиві інформаційного простору, положення Концепції інформаційної безпеки України сприяють формуванню та розвитку інформаційного суспільства, залишаючи поза увагою той факт, що таке суспільство в умовах ведення агресивних війн стає першим об'єктом впливу, забезпечуюючи противнику сприятливі умови гібридного впливу на суспільство, державу і особистість, тобто аквтине та ефективне ведення інформаційних війн.

Наведений підхід має забезпечити протидію комплексу загроз інформаційній безпеці України, що передбачає [1; 2; 10]:

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 інфор-

мації; 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 характеристик; 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 органи 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 інформаційних систем; включення у програмно-технічні засоби прихованих шкідливих функцій тощо.

Як справедливо підкреслюють дослідники, урахування цього потребує вироблення та впровадження конкретних механізмів державного управління у сфері забезпечення національної безпеки, які спрямовані на протидію інформаційно-психологічних загроз [1, с. 122]. У цьому аспекті інформаційна безпека держави має грунтуватись на концептуальному положенні системного підходу до дослідження проблем національної безпеки, на основі якого інформаційна безпека держави у своєму змісті набуває визначальних характеристик ступеня захищеності і стійкості основних сфер життєдіяльності держави і суспільства, що забезпечують резистентну здатність системи протистояти небезпечним (дестабілізаційним, деструктивним) чинникам інформаційного середовища, інформаційним впливам на всіх етапах розповсюдження та обміну інформації.

Висновки. У вирішенні проблем інформаційної безпеки зберігається переважання утилітарного підходу, який поєднує в собі традиційний інформаційний або кібернетичний (фактичне ототожнення поняття інформаційної безпеки із захистом інформації) та політологічний (вивищення компенсаторної функції та принципу гомогенності) підходи до вирішення проблем національної безпеки в цілому та інформаційної безпеки держави зокрема. Водночас поступово відбувається зсув принципових позицій у концептуалізації основних підходів до забезпечення інформаційної безпеки, що дає можливість визначити напрями державної політики у сфері інформаційної безпеки, що є невід'ємною складовою всієї системи забезпечення інформаційної безпеки, набуваючи особливого значення під час війн та суспільних конфліктів.

Список літератури:

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. Вітер Д., Руденко О. Сучасна парадигма протидії загрозам національній безпеці: питання стратегічного управління. *Право та державне управління*, 2022, № 3, С. 220–226.

3. Горник В., Кравченко С. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ ім. В.І. Вернадського. Сер.: Державне управління*, 2020, № 2, Т. 31 (70), С. 206–212.

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

5. Інформаційна безпека держави / В. Гур'єв, Д. Мехед, Ю. Ткач, І. Фірсова. Ніжин: ТПК «Орхідея», 2018, 166 с.

6. Концепція інформаційної безпеки України (Проект). URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

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

8. Стратегічне управління та державне реагування на загрози національній безпеці у сфері безпеки державного кордону: моног. / Д. Вітер та ін. К: НУОУ, 2021. 232 с.

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

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

11. Viter, D. Some issues of the application of special operations forces in multi-domain operations / Theoretical And Applied Aspects Of The Russian-Ukrainian War: Hybrid Aggression And National Resilience, 2023, PP. 209–220.

Zakharov M.V. CONCEPTUALIZATION OF APPROACHES TO ENSURING INFORMATION SECURITY OF THE STATE IN CONDITIONS OF WAR

The article deals with conceptualization of approaches to information security in conditions of martial law and war. Analyze the approaches to determining the content and essence of information security of the state. The need for the formation of 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, is substantiated. It is argued that the principles underlying the draft Concept of Information Security of Ukraine do not fully correspond to the tasks that arise before the state and society in war conditions. By creating general conditions and implementing general principles of ensuring information rights and freedoms, certain regulations of the information space, the provisions of the Information Security Concept of Ukraine contribute to the formation and development of an information society, ignoring the fact that such a society in the conditions of aggressive wars becomes the first an object of influence, providing the enemy with favorable conditions for hybrid influence on society, the state, and the individual, that is, effective and efficient conduct of information wars. In this aspect, it is justified that the information security of the state should be based on the conceptual position of a systemic approach to the study of national security problems, on the basis of which the information security of the state in its content acquires the defining characteristics of the degree of security and stability of the main spheres of life of the state and society, which ensure the system's resilience resist dangerous (destabilizing, destructive) factors of the information environment, informational influences at all stages of dissemination and exchange of information.

Key words: *approach, conceptualization, information security, information security of state, information war, national security, war.*