УДК 355.04: 004.056 https://doi.org/10.33099/2304-2745/2025-3-86/24-32

Саричев Ю. О., кандидат технічних наук, старший науковий співробітник (0000-0003-1380-4959)
Мазуренко І. М., доктор філософії (0000-0003-2233-7563)
Зубков В. П. (0009-0008-5755-2339)
Піщанський Ю. А. (0000-0003-4392-3318)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Загальні передумови досягнення інформаційної переваги під час зародження воєнного конфлікту

Резюме. Обґрунтовано загальні передумови досягнення інформаційної переваги під час зародження воєнного конфлікту. Доведено, що врахування таких передумов дозволяє сформувати вимоги щодо формування системи заходів протидії інформаційним загрозам та нейтралізації негативного інформаційного впливу, зокрема на етапі зародження (виникнення) воєнного конфлікту.

Ключові слова: воєнний конфлікт; інформаційний простір; інформаційна перевага; інформаційна безпека; інформаційна загроза; інформаційний вплив.

Постановка проблеми. Повномасштабна збройна агресія РФ проти України поставила перед дослідниками воєнної сфери багато складних питань, серед яких важливим є дослідження умов зародження та розвитку воєнного конфлікту, що призвели до такої агресії. Зазвичай, воєнні конфлікти виникають внаслідок росту протиріч між суспільними інтересами держав, які відбуваються у економічній, соціальній, інформаційній та воєнно-політичній сферах. Такі протиріччя мають прояв через фактори соціального значення у цих сферах, що і виражають передумови такого конфлікту. Їх виявлення та врахування мають важливе значення для аналізу та подальшої генерації рекомендацій стосовно прийняття рішень щодо подальших дій на всіх етапах ескалації конфлікту: зародження (виникнення), розвиток і припинення.

Загалом, сучасний воєнний конфлікт носить “гібридний” характер з чітко вираженою інформаційною складовою, починаючи з етапу його зародження. При цьому *під зародженням воєнного конфлікту* слід розуміти процес, що передує прямому застосуванню збройної сили та характеризується напруженням між суб’єктами конфлікту, наростанням протиріч, загостренням відносин та, зрештою, переходом до воєнних дій [1]. Розвиток такого явища, зокрема за досвідом подій, що відбуваються в сучасній Україні, показує, що процеси в інформаційній сфері інтенсивно супроводжували зародження (виникнення) воєнного конфлікту. Вже на цьому етапі питання досягнення інформаційної переваги над супротивною стороною є актуальним, передусім для зниження напруження між суб’єктами з подальшим зменшенням протиріч, вирішенням проблемних питань мирним шляхом та недопущенням воєнних дій. Тому це питання потребує окремої уваги та розгляду.

Аналіз останніх досліджень і публікацій. Протягом останніх десятиліть в Україні маємо певну кількість публікацій, дотичних до питання досягнення інформаційної переваги над противником. Серед вітчизняних вчених і фахівців цій темі приділено певну увагу в роботах [2-8], де висвітлюються важливі для досягнення інформаційної переваги питання, як-то:

захист інформаційного простору України;

особливості забезпечення інформаційної безпеки держави у контексті протидії інформаційним війнам;

еволюція форм і способів сучасної інформаційної боротьби у ході підготовки до збройного конфлікту.

Аналіз показав, що ці публікації не враховують особливостей інформаційних процесів на етапі зародження воєнних конфліктів, зокрема, що свідчить про обмеженість таких досліджень і, є недоліком. Ці роботи:

1) присвячені вивченню окремих складових проблем для умов мирного часу і не враховують специфіку часових показників переходу до надзвичайного і воєнного стану;

2) не мають термінологічної єдності уживання базових категорій в описі інформаційних процесів, характерних під час

зародження воєнних конфліктів, що ускладнює їх розуміння;

3) використовують різнорідні підходи при розгляді інформаційних процесів на етапі зародження воєнного конфлікту;

4) не систематизують ознаки процесу зародження воєнного конфлікту, що не дозволяє чітко визначити поточний стан воєнно-політичних, соціально-економічних та інших відносин між суб'єктами конфлікту тощо.

Проте, ознаки процесу зародження воєнного конфлікту проявляються за усіма сферами його протікання: воєнної (воєнно-технічної), політичної, дипломатичної, економічної, соціальної тощо. Законодавство України [9] визначає початковий період зародження воєнного конфлікту як латентну (неактивну) фазу збройного конфлікту – ситуацію, за якої відбувається виникнення суперечностей з приводу визначеного об'єкта (політики, економіки, території тощо), зростання недовіри і напруженості, висування односпрямованих або взаємних претензій, мінімізація контактів, прагнення довести правомірність своїх домагань, звинувачення супротивника в небажанні вирішувати спірні питання "справедливими" методами, замикання на своїх власних стереотипах, упередженість і неприязнь у сфері двосторонніх відносин, виникнення поодиноких збройних інцидентів та збройних провокацій, зокрема на державному кордоні.

Латентна фаза характеризується відсутністю або малою інтенсивністю застосування зброї та може проявлятися з певною періодичністю після активних фаз (загострень) у довготривалих, заморожених конфліктах.

За ознаки зародження воєнного конфлікту може бути прийнято такі стадії:

- напруження – це стадія, коли між суб'єктами конфлікту виникають протиріччя та розбіжності, які можуть бути економічного, соціального, політичного, або навіть культурного характеру;
- посилення напруження – протиріччя загострюються, відносини між суб'єктами конфлікту погіршуються, можуть відбуватися провокації та демонстрація воєнної сили;
- максимальне (пікове) напруження – напруження використовується як інструмент впливу на протиборчу сторону конфлікту, можуть проводитися демонстрації воєнної сили, заявлятися вимоги та погрози;
- підготовка до воєнних дій – суб'єкти конфлікту починають готуватись до збройного протистояння: відбувається мобілізація ресурсів, проводяться бойові злагодження підрозділів та військових частин, накопичується військова техніка та озброєння.

Ключові фактори, що сприяють зародженню воєнного конфлікту:

політичні та територіальні протиріччя – конфлікт може виникати внаслідок суперечностей в політичних системах, територіальних претензіях, або ж в питаннях влади;

економічні інтереси – конфлікт може бути спровокований боротьбою за ресурси, контроль над ринками, або ж економічні розбіжності;

соціальні та культурні розбіжності – національні, релігійні, расові, або ж інші соціальні та культурні відмінності можуть призвести до загострення конфлікту;

нездатність до переговорів та компромісів – відсутність ефективного діалогу та готовності до компромісів може призвести до ескалації конфлікту.

Огляд вищезазначених сфер і факторів вказує на те, що інформаційні процеси є рушійною силою кожного з них. Саме тому такі ознаки найбільш характерно проявляються в інформаційній сфері, проте дослідники не приділяють достатньої уваги цим питанням зародження воєнного конфлікту.

Зазначене свідчить про недосконаліть інформаційної складової теорії воєнних конфліктів. Неврахування особливостей сучасних інформаційних процесів унеможливлює у повній мірі втілювати в життя практичні дії для досягнення інформаційної переваги над противником, зокрема, що вкрай важливо, на етапі зародження воєнного конфлікту.

Все це спричиняє актуальну науково-практичну проблему удосконалення складової теоретичних основ воєнних конфліктів, зокрема яка стосується інформаційної сфери. Вона може бути вирішена шляхом розв'язання низки питань щодо досягнення інформаційної переваги, в тому числі за рахунок врахування сукупності суттєвих факторів інформаційного характеру, перш-за-все на етапі зародження сучасного воєнного конфлікту. Тому одним з напрямків досліджень слід вважати аналіз загальних передумов досягнення інформаційної переваги над противником на цьому етапі в інтересах вирішення проблемних питань мирним шляхом та недопущення воєнних дій.

Виходячи із зазначеного, **метою статті** є визначення передумов досягнення інформаційної переваги над противником в ході зародження воєнного конфлікту шляхом врахування основних факторів інформаційної сфери (наявність релевантної інформації (даних) про суперника, своєчасність та достовірність її отримання, захищеність тощо).

Виклад основного матеріалу. Оскільки існуючі в публікаціях дефініції не враховують особливостей зародження воєнного конфлікту, доцільно сформулювати базові визначення. Взявши за основу стандарт [10], пропонується наступне тлумачення понять.

Інформаційна перевага – перевага над протидіючою стороною в оперативності та якості інформаційного забезпечення процесів державного (військового) управління на свою користь.

Інформаційне забезпечення - сукупність заходів органів державного управління усіх рівнів, дій військ (сил) та інших суб'єктів інформаційної діяльності з метою створення (формування) і використання в інформаційному просторі необхідних інформаційних ресурсів для реалізації процесів державного управління.

Ця перевага може бути також використана для досягнення таких цілей як вплив на громадську думку, воєнний, політичний, дипломатичний або економічний вплив на противника.

Загалом, в сучасному світі чинник інформаційної переваги стає все більш важливим для різних сфер життєдіяльності держави, а саме забезпечує [11]:

у політичній сфері – дієвий контроль над суспільним інформаційним простором, що дозволяє впливати на громадську думку та вибори;

у воєнній сфері – перевагу шляхом здатності оперативно та якісно здійснювати інформаційне забезпечення процесів військового управління з урахуванням інформаційних спроможностей (можливостей) противника;

у економічній сфері – швидкий доступ до інформації та її аналіз, що дає компаніям конкурентну перевагу;

у інформаційній сфері (захисті інформаційних інтересів держави) – інформаційну безпеку держави, що є важливою складовою її національної безпеки.

Відповідно, наростання протиріч по кожній з цих сфер може бути виявлене через певну сукупність ознак процесу зародження воєнного конфлікту. З метою ґрунтовного аналізу ситуації, що склалася в інформаційній сфері України, розглянемо основні аспекти, які супроводжують процес зародження (виникнення) воєнного конфлікту, що є важливим і для теорії, і для практики пошуку шляхів досягнення інформаційної переваги над противником.

Серед таких аспектів доцільно виділити наступні [11]:

моніторинг (пошук) – збір даних про противника, його можливості, плани та слабкі місця;

аналіз даних – їх перетворення на корисні знання (інформацію), які можна використовувати для прийняття рішень;

часові показники – перемога у війні часто залежить від здатності збирати дані та отримувати і використовувати поточну інформацію швидше та ефективніше, ніж противник;

захист інформації – запобігання витоку власної інформації та захист критично важливих об'єктів (систем) інформаційної інфраструктури від руйнування;

кібердії (дії в кіберпросторі) – кіберрозвідка для визначення слабких місць системи (інфраструктури) противника з метою порушення її сталої роботи у випадку початку конфлікту;

інформаційно-психологічні операції – здійснення заходів пропаганди та дезінформації для впливу на противника шляхом поширення певної інформації щодо його дискредитації.

Перелічені аспекти значною мірою є складовими забезпечення інформаційної безпеки держави та суттєво впливають на її рівень. Тому інформаційна перевага у протистоянні неможлива без досягнення сталого рівня інформаційної безпеки будь-якої держави [12], зокрема це актуально і для України. Стаття 17 Конституції України [13] наголошує, що це є найважливішою функцією держави, справою всього Українського народу. Виконання цієї функції вимагає від усіх інститутів держави концентрації зусиль, щоб за потреби мати досягнення інформаційної переваги над противником. Вкрай важливим є вирішення питання інформаційної безпеки держави заздалегідь (превентивно), ще до зародження воєнного конфлікту, спрямованого проти України.

Інформаційна безпека, як важлива функція будь-якої держави, покликана гарантувати сприятливі умови для життя і продуктивної діяльності громадян, державних

інститутів, захищати життєво важливі інтереси людини, суспільства й держави в її інформаційному просторі від зовнішніх і внутрішніх інформаційних загроз. Така захищеність забезпечується відповідним комплексом заходів органів державного управління щодо зменшення або усунення ймовірних загроз інформаційній безпеці (інформаційних загроз).

Наразі керівництво держави приділяє значну увагу питанням досягнення інформаційної переваги над противником. Так, створені основні структурні елементи (органи управління, виконавчі органи, об'єкти впливу, органи моніторингу) системи забезпечення інформаційної безпеки України, розроблений та набрав чинності ряд законодавчих актів України, які стосуються інформаційної сфери [14-23] (закони України, укази Президента України, постанови Кабінету Міністрів України тощо). Ці заходи слід розглядати через призму загального питання досягнення інформаційної переваги.

Водночас, аналіз подій в інформаційній сфері України за цей період свідчить, що окремі складові існуючої системи забезпечення інформаційної безпеки функціонують небездоганно, з різних причин не весь перелік заходів на рівні держави був спланований та виконаний, мали місце непорозуміння, неузгодженість та не координованість дій різних суб'єктів сил оборони України, що негативно впливає на стан досягнення інформаційної переваги.

Детальний аналіз [12] існуючого в законодавстві України [14] визначення інформаційної безпеки показує на певну його недосконаліть, хоча воно може бути взяте за основу власного модифікованого визначення в редакції:

інформаційна безпека України – складова частина національної безпеки України, стан захищеності, за якого запобігається нанесення шкоди життєво важливим інтересам людини, суспільства і держави через:

неповноту, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби;

негативний інформаційний вплив;

нерегульоване або злочинне застосування інформаційних технологій;

несанкціоноване розповсюдження, використання й порушення цілісності інформації та інших ІР з обмеженим доступом;

недосконаліть комунікативної політики держави;

недостатній рівень медіакультури суспільства.

Таке визначення враховує усі фактори інформаційної сфери, що відображають передумови досягнення інформаційної переваги Україною над противником, зокрема в ході зародження воєнного конфлікту.

Посеред основних суттєвих факторів можна вказати на недостатній рівень розвитку теоретичних основ забезпечення інформаційної безпеки держави, який є в Україні, що впливає на досконаліть функціонування існуючої системи забезпечення інформаційної безпеки держави, а це особливо важливо під час зародження воєнного конфлікту. Це не дозволяє якісно, однозначно і зрозуміло для усіх суб'єктів системи планувати практичну діяльність. Наслідком цього практична діяльність дезорієнтується, що призводить до довільного розуміння власних дій, а відповідно і планування та виконання заходів, тобто конкретної діяльності. Особливо негативні наслідки настають у випадку формування та реалізації комплексу заходів державної інформаційної політики, яка концентровано визначається нормами національного законодавства.

Більшість фахівців інформаційної сфери стверджують, що майбутнє збройного протиборства та можливість досягнення інформаційної переваги все більше зміщується у бік інформатизації всіх процесів державного та військового управління, надання інформаційним ресурсам будь-якого (тактичного, оперативного та стратегічного) рівня першочергового значення. Існуючий стан інформаційного простору України в сучасних умовах інформаційного протиборства викликає певну стурбованість із-за його чутливості та уразливості від значної кількості потенційних і реальних інформаційних загроз. При цьому *під інформаційною загрозою державі* слід розуміти наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів) [11].

Аналіз таких загроз показує, що, перш за все, потрібно враховувати умови і чинники, які діють на процес їх виникнення та розвиток. Виходячи з розмаїття і мінливості дій таких факторів, необхідно мати на увазі різнорідність інформаційних ресурсів держави та здатність до їх захисту, складу її інформаційної

інфраструктури, коло можливих змін стану інформаційних загроз, можливість реалізації того або іншого виду загрози тощо. Характеристики інформаційного впливу віддзеркалюють всі основні аспекти функціонування інформаційних загроз. Якщо узагальнити ці інформаційні процеси, то можна визначити динаміку розвитку інформаційного впливу:

чинник інформаційної загрози (виклик) → прояв інформаційної загрози →
→ реалізація загрози (інформаційний вплив) → результати впливу.

Причому, чинники інформаційної загрози не завжди можна одразу виявити та ідентифікувати, вони, як правило, приховані, їх прояв можна оцінити лише за результатами такого впливу. Реалізація таких загроз може викликати:

підрив обороноздатності країни шляхом порушення функціонування об'єктів інформаційних систем органів державного і військового управління, що забезпечують національну безпеку, і як наслідок, позбавлення можливості своєчасної організації оборони держави і досягнення інформаційної переваги над противником;

дезорганізацію роботи систем та засобів інфраструктури критично важливих галузей (фінансового сектора, енергозабезпечення, водопостачання, транспорту і т.п.), що призводить до хаосу в економіці, масовим безладам, зниження промислового, економічного й оборонного потенціалу;

несанкціонований доступ до державних, військових і комерційних конфіденційних даних;

психологічну дію на персонал органів державного і військового управління, деморалізацію населення за рахунок розповсюдження інформації провокаційного або підривного характеру;

примушення до небажаної альтернативи рішення, а в подальшому і до недоцільного варіанта дій шляхом дезінформації.

За результатами такого огляду можна дійти висновку, що найбільш вірогідними чинниками (джерелами зовнішніх загроз) для власного інформаційного простору є сили і засоби недружніх іноземних держав, а також терористичні й злочинні угруповання, агресивні промислово-фінансові групи, хакери. Крім того, не слід виключати можливість виникнення внутрішніх загроз і зі сторони співробітників власних установ та підрозділів.

Тому більш детально зупинимося на групі факторів державного рівня, зокрема пов'язаних з існуванням загроз інформаційного характеру під час процесу зародження (виникнення) воєнного конфлікту та необхідністю їх нейтралізації. Серед таких загроз найбільш небезпечними є наступні:

зовнішні загрози:

усі види розвідувальної діяльності ззовні, спрямованої на доступ до інформаційних ресурсів держави у воєнній сфері;

інформаційно-технічні впливи на інформаційну інфраструктуру суб'єктів сил оборони України та інформаційні ресурси у воєнній сфері з метою порушення їх дієздатності, виведення із ладу або знищення;

інформаційно-психологічні впливи на керівний (особовий) склад суб'єктів сил оборони України, як у мирний час, так і під час зародження воєнного конфлікту;

міжнародна інформаційна діяльність іноземних політичних, економічних і воєнних структур, яка спрямована проти національних інтересів держави у воєнній сфері, приниження її міжнародного іміджу;

наявність на озброєнні армій іноземних держав високоточної зброї, зокрема, самонавідної на радіовипромінювання, як засобу вогневого ураження елементів інформаційної інфраструктури суб'єктів сил оборони України;

внутрішні загрози:

недосконаліть нормативно-правової бази держави у сфері національної безпеки, у тому числі законодавча невизначеність щодо повного переліку суб'єктів сил оборони України, розподілу їх функцій, завдань і механізмів взаємодії при підготовці та веденні воєнних дій;

відсутність єдиної (інтегрованої) інформаційної інфраструктури суб'єктів сил оборони України, відомчий характер політики та заходів щодо забезпечення інформаційної безпеки;

нездатність сил оборони України в межах його інформаційної інфраструктури реалізувати весь перелік основних інформаційних процесів, необхідних для забезпечення достатності (повноти) інформаційного простору держави в умовах сучасного воєнного конфлікту;

обмежені спроможності держави упродовж конкретної кризової ситуації підтримувати сталість створеної інформаційної інфраструктури її сил оборони України шляхом всебічного ресурсного забезпечення

(матеріально-технічного, фінансового, кадрового, медичного), а також здійснити захист цієї інфраструктури від фізичного знищення засобами вогневого ураження противника;

відсутність розуміння необхідності впровадження концепції "управління противником" у воєнному конфлікті як ідеологічної бази військового будівництва та підготовки сил оборони України до захисту від зовнішньої агресії в умовах сучасної війни та війн майбутнього, що перешкоджає організації основних інформаційних процесів та їх взаємозв'язку для формування єдиного інформаційного простору держави у воєнній сфері;

недосконаліть комплексної системи захисту інформаційних ресурсів, доступних для елементів інформаційної інфраструктури сил оборони України;

зловмисні та невмотивовані (випадкові) шкідливі дії персоналу (особового складу) інформаційної інфраструктури сил оборони України;

нерозвиненість наукових основ підготовки та проведення інформаційних операцій елементами інформаційної інфраструктури сил оборони України в умовах воєнного конфлікту;

слабкість державницької ідеології, освітянської, виховної та адміністративної практики, спрямованих на зміцнення патріотичної свідомості громадян, а також забезпечення психологічної стійкості персоналу (особового складу) структур суб'єктів сил оборони України у воєнному конфлікті;

неналежний рівень професійної підготовки персоналу (особового складу) інформаційної інфраструктури сил оборони України, особливо у ланці керівних органів;

недостатність міжнародної інформаційної діяльності держави щодо формування її позитивного іміджу у воєнній сфері, а також проведення заходів контрпропаганди у міжнародному інформаційному просторі.

Реалізація описаних вище загроз, в тому числі під час зародження воєнного конфлікту, може здійснюватися різними способами втручання в наявні інформаційні ресурси та роботу систем та засобів інформаційної інфраструктури. Серед них на сьогодні можна виділити такі:

навмисне фізичне пошкодження або руйнування апаратних засобів, модифікація повідомлень та даних, перевантаження мереж обміну інформацією, маршрутизаторів або серверів інформаційно-керуючих систем;

внесення змін до функціонування системи (порушення логіки роботи, помилкова відмова в доступі або квитанції);

втручання зсередини (перегляд і розкрадання трафіку й даних);

перехоплення інформації, що передається, дослідження запитів до бази даних і їх криптографічний аналіз.

Нейтралізація зазначених загроз може бути здійснена шляхом реалізації виваженої державної інформаційної політики, спрямованої на проведення в життя комплексу заходів щодо створення та розвитку єдиного інформаційного простору України, зокрема у воєнній сфері (силах оборони), та його всебічного захисту від *негативного інформаційного впливу*, що потребує визначення відповідних концептуальних засад забезпечення інформаційної безпеки України у воєнній сфері.

Загалом, *під інформаційним впливом* слід розуміти організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій [8,10]. Головною метою здійснення деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури, зокрема воєнної сфери, є досягнення переваги в умовах інформаційного протиборства шляхом дестабілізації або виведення з ладу системи військового управління противника, а також деморалізації особового складу його військ (сил). При цьому засобами інформаційного впливу є засоби масової інформації, лінгвістичні, програмні, технічні та інші спеціальні засоби, які призначені для реалізації інформаційного впливу.

Інформаційний вплив поділяється на інформаційно-технічний та інформаційно-психологічний.

Інформаційно-технічний вплив – цілеспрямоване втручання в процес функціонування технічних об'єктів інформаційної інфраструктури та фізичний стан людини шляхом застосування засобів і технологій радіоелектронного впливу та кібернетичної зброї [10]. Його результатом може бути дестабілізація інформаційної діяльності об'єкту впливу внаслідок пошкодження, викривлення, руйнування, блокування інформаційних ресурсів або виведення об'єкту з ладу шляхом:

використання комп'ютерних "вірусів" (комп'ютерних програм для деструктивної зміни програмного забезпечення ПЕОМ та комп'ютерних мереж);

застосування "комп'ютерних бомб" (спеціальних комп'ютерних закладних програм руйнівного характеру);

поширення фальшивої інформації в комп'ютерних мережах;

обмеження або заборони доступу до інформаційних ресурсів законним користувачам комп'ютерних мереж;

програмного ураження інформаційно-телекомунікаційних систем з боку вітчизняних комп'ютерних злочинців або хакерів противника;

ненавмисного порушення встановленого порядку роботи з інформаційними ресурсами персоналом (особовим складом) інформаційної інфраструктури;

радіоелектронного придушення радіотехнічних засобів (зв'язку, спостереження, навігації, радіо, телебачення);

зміни фізичного або психічного стану людини.

Деструктивний інформаційно-технічний вплив, зокрема, може бути спрямований на такі об'єкти в інформаційній інфраструктурі воєнної сфери, як: інформаційно-телекомунікаційні мережі (комп'ютерні мережі та засоби зв'язку, електронні засоби масової інформації; електронні архіви (сховища) та банки даних і знань довготривалого зберігання; засоби автоматизації систем управління військами та зброєю; радіоелектронні засоби і системи (навігації, спостереження, армійські радіостанції, телебачення тощо); інформація, що циркулює на об'єктах інформаційної інфраструктури в реальному часі; людина (соціальні групи) безпосередньо.

Інформаційно-психологічний вплив – цілеспрямоване інформаційне втручання у свідомість (підсвідомість) цільової аудиторії з метою корекції її поведінки та (або) світогляду, зміни морально-психологічного стану [10].

Засобами інформаційно-психологічного впливу є засоби масової інформації, спеціальна друкована продукція, публічна голосова агітація, агентурна діяльність, спеціальні інформаційні технології тощо. Його результатом може бути внесення негативних змін у свідомість та морально-психологічний стан особового складу військових формувань, керівництва та населення держави-противника, що також впливає на досягнення над ним інформаційної переваги.

Для визначення рівня деструктивного інформаційного впливу на цільові об'єкти на рівні держави необхідно мати систему оцінювання такого впливу з певною сукупністю показників, а для визначення його значимості – відповідні критерії. Відмітимо, що одним із підходів для отримання якісних оцінок деструктивного інформаційного впливу на наявні інформаційні ресурси та елементи інформаційної інфраструктури може бути застосування методів експертного оцінювання, які враховують досвід фахівців інформаційної сфери, в тому числі під час зародження воєнного конфлікту. На основі цього підходу запропоновано реалізувати базові методичні елементи для такого оцінювання, які описані, зокрема, в роботах [24,25].

Таким чином, наведений аналіз умов і чинників та їх деталізація дозволяють сформулювати передумови досягнення інформаційної переваги над противником в ході зародження воєнного конфлікту. Зазначене досягається шляхом забезпечення інформаційної безпеки держави – координованого комплексного процесу недопущення збитковості в інформаційному просторі держави як реалізація запобіжних заходів проти нанесення шкоди у різних галузях життєдіяльності із-за актуальних загроз її інформаційній безпеці (намірів, що передбачають вчинення деструктивних дій в інформаційному просторі; вчинення деструктивних дій в інформаційному просторі; власної бездіяльності в інформаційному просторі; непереборних явищ (процесів) в інформаційному просторі).

Серед таких заходів слід виділити наступні, що формують кібернетичний контур управління [26] щодо досягнення інформаційної переваги:

моніторинг та збір даних про противника;

кіберрозвідка для визначення слабких місць системи (інфраструктури) противника з метою порушення її сталої роботи у випадку початку конфлікту;

аналіз даних та їх перетворення на інформацію;

використання отриманої інформації для прогнозування можливих дій ймовірного противника;

захист інформації для запобігання її витоку;

недопущення ураження критично важливих об'єктів власної інформаційної інфраструктури;

здійснення заходів пропаганди та дезінформації для впливу на противника шляхом поширення певної інформації щодо його дискредитації.

Висновки. Досягнення інформаційної переваги дає можливість під час зародження воєнного конфлікту знизити напруження між суб'єктами воєнного конфлікту з подальшим зменшенням протиріч, вирішенням проблемних питань мирним шляхом та недопущенням воєнних дій. Головною передумовою інформаційної переваги є досягнення сталого рівня інформаційної безпеки держави, який гарантує необхідний стан захищеності інформаційного простору держави в умовах впливу внутрішніх та зовнішніх інформаційних загроз.

Подальші дослідження слід зосередити на розробці пропозицій щодо формування та реалізації виваженої державної інформаційної політики, спрямованої на досягнення необхідного рівня інформаційної безпеки держави в інтересах інформаційної переваги, зокрема шляхом впровадження комплексу заходів для створення та розвитку єдиного інформаційного простору України та його всебічного захисту від негативного інформаційного впливу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Магда Є.В. Гібридна агресія Росії: уроки для Європи / Є.В. Магда. – К.: Каламар, 2017. – 268с.
2. Богуш В.М. Основи інформаційної безпеки держави: Вступ до спеціальності / В.М. Богуш, О.К. Юдін – Харків: Консум, 2004. – 439 с.
3. Інформаційна безпека держави: навч. посібник / О.К. Юдін, В.М. Богуш. – Х.: Консум, 2005. – 576 с.
4. Проблеми захисту інформаційного простору України: Монографія / В.П. Горбулін, М.М.Биченок / Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.
5. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: Монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: "Інтертехнологія", 2009. – 164 с.
6. Інформаційна безпека держави у контексті протидії інформаційним війнам. Навчальний посібник / [за ред. В.Б. Толубка]. – К.: НАОУ. – 2004. – 315 с.
7. Руснак І.С., Телелим В.М. Розвиток форм і способів інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С.18-23.
8. Левченко О.В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та застосування: монографія / О.В. Левченко. – Житомир: Видавець ПП "Євро-Волинь", 2021. – 172 с.
9. Постанова Кабінету Міністрів України від 22 липня 2020 року № 636 "Про затвердження Порядку розроблення Плану оборони України". – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/636-2020-%D0%BF/conv#Text.
10. Військовий стандарт. Інформаційна безпека держави у воєнній сфері. Терміни та визначення: ВСТ 01.004.004 – 2014 (01). – [Чинний від 2014 – 02 – 27]. – К.: МОУ, 2014. – 22 с.
11. Горбулін В.П. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. – К.: НІСД, 2017. – 496 с.
12. Інформаційна безпека України у воєнній сфері: засадничі елементи становлення теоретичних основ її забезпечення: монографія / В.В. Грицюк, І.В. Єфіменко, В.П. Зубков, В.В. Машталір, С.А. Микусь, А.К. Павліковський, Ю.А. Піщанський, Ю.О. Саричев, П.М. Сніцаренко, В.А. Ткаченко [за заг. ред. П.М. Сніцаренка, 2-е вид., допов.]. – К.: НУОУ, 2025. – 300 с.
13. Конституція України. Прийнята ВР України 28.06.1996 р.
14. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 р. № 537-V // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon3.rada.gov.ua.
15. Закон України "Про інформацію" в редакції від 13.01.2011 р. № 2938-VI // Законодавство України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua.
16. Закон України "Про телекомунікації" від 18.11.2003 р. № 1280-IV // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon2.rada.gov.ua.
17. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon2.rada.gov.ua.
18. Стратегія національної безпеки України: Указ Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу: http: // zakon5.rada.gov.ua.
19. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021 Про рішення РНБО України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.
20. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.
21. Про невідкладні заходи з кібероборони держави: Указ Президента України від 26 серпня 2021 року № 446/2021 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.
22. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Указ Президента України від 19 березня 2022 року № 152/2022

[Електронний ресурс]. – Режим доступу: http: // president.gov.ua.
23. Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р “Про схвалення Стратегії розвитку інформаційного суспільства в Україні” [Електронний ресурс]. – Режим доступу: http: // zakon.rada.gov.ua.
24. Методичний підхід до виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П.М.Сніцаренко, Ю.О.Саричев, Ю.І.Міхєєв, М.В.Праута // Наука і оборона. – № 3-4. – 2017. – С.18-25.
25. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П.М. Сніцаренко, Ю.О. Саричев, В.А. Ткаченко, Л.В. Хоменко // Наука і оборона. – № 2. – 2018. – С.40-45.
26. Винер Н. Кибернетика или управление и связь в животном и машине / Н. Винер. – М.: Сов.радио, 1968. – 328 с.

Стаття надійшла до редакції 25.07.2025

General preconditions for achieving information superiority during the onset of military conflict

Annotation

The onset of military conflict should be understood as the process preceding the direct use of armed force and characterized by tension between the parties to the conflict, growing contradictions, escalating relations, and, ultimately, the transition to military action. The development of this phenomenon, particularly based on the experience of events taking place in modern Ukraine, shows that processes in the information sphere intensively accompanied the emergence (onset) of military conflict. Already at this stage, the issue of achieving information superiority over the opposing side is relevant, primarily to reduce tensions between the parties, followed by a reduction in contradictions, the peaceful resolution of problematic issues, and the prevention of military action.

The purpose of this article is to identify the preconditions for achieving information superiority over the enemy during the emergence of a military conflict by taking into account the main factors in the information sphere: the availability of relevant information (data) about the opponent, the timeliness and reliability of its acquisition, security, etc.

The analysis of conditions and factors and their detailing allow us to formulate the preconditions for achieving information superiority over the enemy during the onset of a military conflict. This is achieved by ensuring the information security of the state – a coordinated comprehensive process of preventing losses in the information space of the state as the implementation of preventive measures against damage in various areas of life due to current threats to its information security. The main precondition for information superiority is the achievement of a stable level of state information security, which guarantees the necessary state of protection of the state's information space in the face of internal and external information threats.

Keywords: military conflict; information space; information superiority; information security; information threat; information influence.