

## АНАЛІЗ ЗАГРОЗ ВОЄННОЇ БЕЗПЕКИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ ТА ПРОТИДІЇ ЇМ В УМОВАХ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ

*У статті розглянуто загрози інформаційної безпеки України в контексті інформаційної війни, які застосовуються для впливу на свідомість населення. Встановлено, що нові тенденції в методах ведення сучасних інформаційних воєн, викликані розвитком інформаційних технологій, настільки масштабні, що дозволяють військовим аналітикам говорити про новий напрямок у військовій справі. На сьогодні інформаційна боротьба стає однією з важливих, а не рідка й основних форм вирішення суперечностей між державами, і в цій боротьбі шляхом проведення інформаційних операцій досягаються стратегічні цілі. Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. Визначено, що найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційні.*

*Визначено, що на сьогодні інформаційна боротьба стає однією з важливих та основних форм вирішення суперечностей між державами. Ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці у воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні.*

*Ключові слова: загрози воєнної безпеки, інформаційна сфера, інформаційна війна, інформаційна безпека.*

**Вступ.** В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин [1]. Глобальна інформатизація і розвиток Інтернету привели до того, що інформаційна інфраструктура країн і національних інформаційних ресурсів виявилися досить уразливими об'єктами впливу з боку іноземних держав, терористичних організацій, кримінальних груп і окремих зловмисників.

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних воєн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації. Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив,

негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [1-3].

**Аналіз останніх досліджень і публікацій, постановка задачі.** Результати аналізу останніх досліджень та публікацій засвідчують, що глобальна інформатизація суспільства стрімкий розвиток інформаційної техніки й нових інформаційних технологій, збільшення суспільства в потребах різноманітних інформаційних послугах зумовили появу нового терміну – інформаційна війна [1-3], яка потребує подальшому вивченню. В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави. Однак саме через інформаційне середовище найчастіше здійснюються загрози воєнної безпеки. Загроза міжнародного інформаційного тероризму й інформаційних воєн стали невід’ємними геополітичними факторами. Тому виявлення й аналіз загроз інформаційної безпеки України, вироблення і вживання заходів, необхідних для адекватної відповіді на них, повинні розглядатися як найважливіші пріоритети національної безпеки.

**Мета статті** – дослідити загрози воєнної безпеки в контексті інформаційної війни. Визначити ролі та місця інформаційної безпеки в системі воєнної безпеки держави, виявити характерні особливості забезпечення інформаційної безпеки держави у воєнній сфері.

**Виклад основного матеріалу.** У сучасних реаліях Україна стикається з серйозними загрозами своїй безпеці. Агресія з боку Росії дестабілізує ситуацію в Україні і становить небезпеку для сусідніх країн. "У конфлікті з Росією Україна змушена реагувати на загрози національній безпеці в трьох вимірах. По-перше, – це військовий конфлікт. Очевидно, що існує військовий вимір в цьому конфлікті, адже за останні 3 роки більше 10 тис. убитих, 1,6 млн внутрішньо переміщених осіб і більше 1 млн біженців в сусідніх країнах", – сказав Мінгареллі в ході круглого столу на тему "Загрози безпеці України та інших країн регіону Східного партнерства і можливі відповіді на них". Він додав, що другий вимір – це економічний, адже в ході окупації Донбасу українська економіка ослабла. Третій вимір – дезінформаційна кампанія з боку РФ.

Активне розроблення інформаційної зброї і підготовка до інформаційних війн багато в чому визначаються поглядами розвинутих країн на цілі, умови, форми і наслідки застосування воєнної сили. Глобальні комп'ютерні мережі видозмінили комунікативні технології спеціального впливу на особистість. Комп'ютерні мережі стали новим етапом у розвитку зовнішніх засобів інтелектуального спілкування та пізнання. Застосування Інтернет-технологій може викликати значні структурні та функціональні зміни у свідомості та психічній діяльності людини, такі технології роблять інтернет новим складним об'єктом інформаційного впливу на суспільство. Сучасними Інтернет-технологіями відпрацьовані й апробовані ефективні методи інформаційних впливів на особистість. Спеціальні впливи можуть бути спрямовані як на суспільство, так і на окремі його групи. Інформаційна сфера все більш перетворюється в арену міжнародного суперництва, що створює небезпеку для національних інтересів. Для боротьби з такими загрозами актуальною є розробка нових засобів захисту інформації, заснованих на методах оперативної ідентифікації потенційних вразливостей, що виникають як на рівне процесів контролю до ресурсів, так і на рівне системних викликів [2-4].

Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Можна констатувати, що: український інформаційний простір є незахищеним від зовнішніх негативних пропагандистське-маніпулятивних впливів і стає об'єктом інформаційної експансії; у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні; діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та

позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення.

Інформаційні війни відносяться до нових категорій конфліктного спектра, що розмиває кордони і предметні сфери традиційних понять економічного, військово-політичного і соціального конфліктів. У ХХІ столітті інформація стає однією з головних цілей ведення бойових дій.

Нові тенденції в методах ведення сучасних інформаційних воєн, викликані розвитком інформаційних технологій, настільки масштабні, що дозволяють військовим аналітикам говорити про новий напрямок у військовій справі. Сутність його полягає не тільки в кількісному нарощуванні технічних характеристик озброєнь і появі нових технологічних рішень вже існуючих завдань у забезпеченні національної безпеки, але і в трансформації способів і методів застосування окремих типів озброєнь і їхніх комбінацій, структури і форм організації військової справи, в новому розумінні мети та задач оборонної політики.

У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни [3]:

1. Поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
2. Зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет;
3. Деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України;
4. Прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками.

Як зазначає Р.Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя [4].

До загроз національній безпеці України в інформаційній сфері також варто зарахувати [5]:

1. Прояви обмеження свободи слова та доступу громадян до інформації;
2. Викривлення, спотворення, блокування, замовчування упереджене та тенденційне висвітлення інформації;
3. Несанкціоноване її поширення;
4. Відкрити дезінформацію;
5. Інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш потужної держави;
6. Виникнення і функціонування у національному інформаційному просторі держави невідконтрольних й інформаційних потоків;
7. Поширення засобами масової інформації культу насильства, жорстокості;
8. Повільність входження України у світовий інформаційний простір;
9. Не виваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері;
10. Розміщення дезінформації в Інтернеті.

В умовах глобалізації небезпечний розвиток регіональних суперечностей, кризових ситуацій та локальних конфліктів дуже швидко позначається на світових процесах

міжнародної безпеки, а отже, вкрай необхідним є зміцнення безпеки і стабільності в кожній частині світу та окремому регіоні.

Під час розроблення спільної стратегії розвитку системи безпеки як інтегрального чинника комплексної системи загальноєвропейської безпеки необхідно враховувати весь спектр загроз національній безпеці держав регіону, зокрема [6]: застосування Росією проти України нового типу агресії, яка має латентний характер, з метою підризу внутрішньої стабільності у спосіб застосування економічного тиску, експорту тероризму, масованої інформаційно-пропагандистської кампанії тощо; наявність у регіоні «заморожених» конфліктів, можливість дестабілізації ситуації на територіях з невизначеним статусом з подальшим переростанням у збройне протистояння; відсутність ефективних механізмів урегулювання регіональних конфліктів, неможливість існуючих міжнародних структур безпеки оперативне реагувати на кризові ситуації; відсутність єдиної позиції країни щодо протидії проявам агресії з боку інших країн; нерівномірний розвиток економік країн регіону, низка з яких досі перебувають під впливом відсталих економічних моделей, різний ступінь розвитку демократичних процесів у цих країнах, що є вагомим гальмуючим чинником процесів чорноморської інтеграції, зокрема і у сфері безпеки; поширення транснаціональних загроз у регіоні: нелегальна міграція, торгівля людьми, розповсюдження зброї масового ураження, нелегальна торгівля зброєю, контрабанда наркотичних речовин, вияви міжнародного тероризму, діяльність транснаціональних злочинних організацій, забруднення навколишнього середовища, надмірне споживання енергетичних, водних та інших ресурсів; ускладнення, пов'язані з розбудовою регіональної транспортної інфраструктури (зокрема створення єдиного транспортного кола навколо Чорного моря) через регіональні суперечності та конфлікти, неможливість забезпечити безпеку транспортних комунікацій; відсутність надійних механізмів гарантування безпеки постачання каспійських енергоресурсів до України та країн ЄС, що є важливим для диверсифікації джерел постачання енергоносіїв та енергетичної безпеки регіону і Європи загалом.

На сьогодні інформаційна боротьба стає однією з важливих, а не рідка й основних форм вирішення суперечностей між державами, і в цій боротьбі шляхом проведення інформаційних операцій досягаються стратегічні цілі.

У військовій справі рівень інформаційного потенціалу обумовлює оперативність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння. Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційна.

З інших загроз стабілізації воєнно-політичної обстановки та недопущення збройних конфліктів в Центральній Європі розглядаються такі [7-8]:

1. Висунення територіальних претензій до України;
2. Втручання у внутрішні справи України;
3. Нестабільність воєнно-політичної обстановки навколо України;
4. Активізація сепаратистських сил і підтримання їх ззовні;
5. Заяви та акції, що дискредитують внутрішню і зовнішню політику України;
6. Войовничість політичного керівництва сусідніх країн;
7. Загострення міжетнічних і міжконфесійних суперечностей;
8. Нестабільність соціально-політичної обстановки в суміжних з Україною країн.

Не виникає сумніву в тому, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома. Крім того, на основі аналізу іноземного впливу на інформаційний медіа та кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції [9-10]: цілеспрямоване формування окремими іноземними державами негативного міжнародного

іміджу України; активізація критики вищого державного керівництва України; здійснення рядом зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах; посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі; дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва; зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Однією з істотних загроз підтримувannya боєздатності військових формувань є втрата престижності воєнної служби і зниження морально-психологічного рівня особового складу. Ця загроза має інформаційний характер.

Виявлення й аналіз загроз інформаційної безпеки України, вироблення і вживання заходів, необхідних для адекватної відповіді на них, повинні розглядатися як найважливіші пріоритети національної безпеки. Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян [11].

Як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямками державної інформаційної політики мають бути [12-13]:

1. Інтеграція України до світового та регіонального європейського інформаційного простору;
2. Інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації;
3. Створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства;
4. Модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;
5. Удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів;
6. Розвиток національної інформаційної інфраструктури;
7. Підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг;
8. Впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління;
9. Ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування та реалізації державної політики в інформаційній сфері.

Жодну війну нині не можна виграти, доки не буде отримано перемогу на інформаційному фронті. Можна мати чи отримати надсучасну зброю, виграти бій, але остаточної перемоги у війні без перемоги на інформаційному фронті боротьби за суспільну свідомість здобути неможливо. В умовах сучасних інформаційних протистоянь, експансіоністської політики Російської федерації, національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів, загроз.

#### **Висновки**

1. Виявлення й аналіз загроз інформаційної безпеки України, вироблення і вживання заходів, необхідних для адекватної відповіді на них, повинні розглядатися як найважливіші пріоритети національної безпеки

2. На сьогодні інформаційна боротьба стає однією з основних форм вирішення суперечностей між державами.

3. Сформовані основні напрямки протидії негативним інформаційно-психологічним впливам. Також одним з пріоритетних напрямків роботи інформаційних структур мають бути: контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій.

#### ЛІТЕРАТУРА:

1. Ільницька У.В. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. [Електронний ресурс] / Ільницька Ульяна – Режим доступу: [science.lpnu.ua/sites/default/files/journal.../ilnicka0.pdf](http://science.lpnu.ua/sites/default/files/journal.../ilnicka0.pdf) (дата звернення 30.08.2018)

2. Адашків О.І. Рекомендації щодо проведення інформаційних заходів в мережі інтернет в інтересах виконання завдань інформаційно психологічних операцій. / Збірник наукових праць військового Інституту Київського національного університету імені Тараса Шевченка. - № 45 – К.: ВІКНУ, 2014. – С. 57 – 67.

3. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25 лютого 2017 року) : [Електронний ресурс] / Офіційне представництво Президента України. – Режим доступу : <http://www.president.gov.ua/documents/472017-21374> (дата звернення 27.08.2018).

4. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: [http://www.dsaua.org/index.php?option=com\\_content&view=article&id=198%3A2014-0813-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk](http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-0813-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk);

5. Почепцов Г. Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2015. – 497 с.

6. “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: <http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14>.

7. Дмитренко М. А. Спеціальні інформаційні впливи // Збірник наукових праць Інституту СЗРУ – 2014. - № 8. – С. 156-167.

8. Косоков О.М. Модель динаміки зміни рівня інформаційної безпеки системи / О.М. Косоков // Зб. наук. праць. – К.: ЦВСД НУО імені І. Черняхівського, 2015. – №2 (54). – С. 76-79.

9. Певцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у військовій сфері / Г.В. Певцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 2 (92). – С. 57-59.

10. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн. / І. О. Валюшко // Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія: традиції, тренди, досвід. Серія «Політичні науки» / За заг. ред. В.Г. Ціватого, Н.О. Татаренко. – 2016. – Випуск 23. Частина II. – С. 142–147.

11. Дмитренко М. А. Спеціальні заходи впливу як механізм протистояння зовнішньополітичним впливам в інформаційних війнах // Збірник наукових праць Інституту Служби зовнішньої розвідки України. – 2016. – № 12. – С. 21 – 37.

12. Левченко О. В. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю. Радковець, О. Левченко, О. Косоков // Наука і оборона. – 2014. – № 1. – С. 38-42.

13. Ленков С.В. Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовищі хмарних обчислень. / В.М. Джулій, О.В. Селюков, І.В. Муляр //Збірник наукових праць військового Інституту Київського національного університету імені Тараса Шевченка. - № 55 – К.: ВІКНУ, 2017. – С. 145-155.

#### REFERENCES:

1. Il'nyts'ka, U.V., (2016) Informatsijna bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnyim informatsijno-psykholohichnym vplyvam. [Information security of Ukraine: modern challenges, threats and mechanisms of counteraction to negative informational and psychological influences.] [science.lpnu.ua/sites/default/files/journal.../ilnicka0.pdf](http://science.lpnu.ua/sites/default/files/journal.../ilnicka0.pdf) (Accessed 30 August 2018)

2. Adas'kov, O.I. (2014) Rekomendatsii schodo provedennia informatsijnykh zakhodiv v merezhi internet v interesakh vykonannia zavdan' informatsijno psykholohichnykh operatsij. [Recommendations for holding information events on the Internet in the interests of performing tasks of information psychological operations.]. Zbirnyk naukovykh prats' vijs'kovoho Instytutu Kyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. Kiev. Trudy universytetu. no 45, pp.. 57 – 67.

3. Doktryna informatsijnoi bezpeky Ukrainy (zatverdzhena ukazom Prezydenta Ukrainy №47/2017 vid 25 liutoho 2017 roku). Ofitsijne predstavnytstvo Prezydenta Ukrainy. <http://www.president.gov.ua/documents/472017-21374> (Accessed 27 August 2018).
4. Marutian, R. R. Rekomendatsii schodo vdoskonalennia polityky zabezpechennia informatsijnoi bezpeky Ukrainy. [Recommendations for improving the policy of ensuring information security of Ukraine] [http://www.dsaua.org/index.php?option=com\\_content&view=article&id=198%3A2014-0813-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk](http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-0813-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk). (Accessed 28 August 2018)
5. Pocheptsov, H. H. (2015) Suchasni informatsijni vijny. [Modern information wars] Kiev. Vyd.dim "Kyievo-Mohylians'ka akademiia", 497 p.
6. Pro zakhody schodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsijnoi bezpeky Ukrainy [On measures to improve the formation and implementation of state policy in the field of information security of Ukraine] Rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r. <http://www.zakon5.rada.gov.ua/laws/show/n0004525-14>. (Accessed 4 September 2018)
7. Dmytrenko, M. A. (2016) Spetsial'ni zakhody vplyvu iak mekhanizm protystoiannia zovnishn'opolitychnym vplyvam v informatsijnykh vijnakh. [Special measures of influence as a mechanism of confrontation with foreign policy influences in information wars]. Zbirnyk naukovykh prats' Instytutu Sluzhby zovnishn'oi rozvidky Ukrainy. no 12. pp. 21 – 37.
8. Kosohov, O.M. (2015) Model' dynamiky zminy rivnia informatsijnoi bezpeky systemy. [The dynamics model changes the level of information security system] Kiev. Zb. nauk. prats'. TsVSD NUO imeni I. Cherniakhovs'koho, no. 2 (54). pp. 76-79.
9. Pievtsov, H.V., Zalkin S.V., Feklistov A.O. (2011) Kontseptual'ni pidkhody schodo zabezpechennia informatsijnoi bezpeky u voiennij sferi. [Conceptual approaches to providing information security in the military sphere]. Kiev. Systemy obrobky informatsii. KhUPS, no. 2 (92). pp. 57-59.
10. Valiushko, I. O. (2016) Osnovni vyklyky i zahrozy v epokhu informatsijnykh vijn. [The main challenges and threats in the era of information wars.] Naukovyj visnyk Dyplomatychnoi akademii Ukrainy. Zovnishnia polityka i diplomatiia: tradytsii, trendy, dosvid. Vypusk no. 23. Chastyna II, pp. 142–147.
11. Dmytrenko, M. A. (2014) Spetsial'ni informatsijni vplyvy. [Special informational impacts] Zbirnyk naukovykh prats' Instytutu SZRU, no. 8, pp. 156-167.
12. Levchenko, O.V., Yu. Radkovets', O. Kosohov. (2014) Pohliady na stvorennia systemy informatsijnoi bezpeky Ukrainy ta ii Zbrojnykh Syl [Views on the creation of the information security system of Ukraine and its Armed Forces]. Nauka i oborona, no. 1, pp. 38–42.
13. Lienkov, S.V., Dzhulij, V.M., Seliukov, O.V. , Muliar, I.V. (2017) Metod predykatyvnoi identyfikatsii protsesiv dlia zakhystu vid prykhovanykh zahroz v seredovysche khmarnykh obchyslen'. [The method of predictive identification of processes to protect against hidden threats in the cloud computing environment.] Kiev. Zbirnyk naukovykh prats' vijs'kovoho Instytutu Kyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka, no. 55, pp. 145-155.

к.воен.н. Никифоров Н.Н., к.т.н., доц. Пампуха И.В., к.т.н. Лоза В.Н.  
**АНАЛИЗ УГРОЗ ВОЕННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В  
 ИНФОРМАЦИОННОЙ СФЕРЕ И ПРОТИВОДЕЙСТВИЯ ИМ В УСЛОВИЯХ ВЕДЕНИЯ  
 ГИБРИДНОЙ ВОЙНЫ**

*В статье рассмотрены угрозы информационной безопасности Украины в контексте информационной войны, применяемые для воздействия на сознание населения. Установлено, что новые тенденции в методах ведения современных информационных войн, вызванные развитием информационных технологий, столь масштабные, позволяющие военным аналитикам говорить о новом направлении в военном деле. Сегодня информационная борьба становится одной из важных, и основных форм разрешения противоречий между государствами, и в этой борьбе путем проведения информационных операций достигаются стратегические цели. Значимость информационной безопасности как составляющей военной безопасности Украины объясняется зависимостью реализации наиболее важных интересов Украины в военной сфере от информационных угроз. Определено, что существенной угрозой национальной безопасности Украины в информационной сфере является осуществление иностранными государствами негативного информационно-психологического воздействия на общественное сознание граждан Украины и мировую общественность через проведение информационных акций и кампаний,*

специальных информационных операций. Значимость информационной безопасности как составляющей военной безопасности Украины объясняется зависимостью реализации наиболее важных интересов Украины в военной сфере от информационных угроз. Из анализа наиболее опасных угроз важным национальным интересам Украины в военной сфере следует, что реализационной основой большинства этих угроз являются. Определено, что на сегодня информационная борьба становится одной из важных и основных форм разрешения противоречий между государствами. Эффективность своевременного выявления и нейтрализации рассмотренных угроз национальной безопасности в военной сфере существенно зависит от взвешенности и активности мероприятий по обеспечению военной безопасности на информационном уровне.

*Ключевые слова:* угрозы военной безопасности, информационная сфера, информационная война, информационная безопасность.

Ph.D. Nikiforov N.N., Ph.D. Pampukha I.V., Ph.D. Loza V.M.

#### ANALYSIS OF THREAT OF MILITARY SECURITY OF THE STATE INFORMATION SCOPE AND COMBATING IT IN THE CONDITIONS OF THE HYBRID WAR

*The article deals with the threats of information security of Ukraine in the context of information warfare, which are used to influence the consciousness of the population. It is established that new trends in the methods of conducting modern information wars, caused by the development of information technology, are so extensive that they allow military analysts to talk about a new direction in military affairs. Today, information struggle is becoming one of the important and not the rare and basic forms of resolving conflicts between states, and in this struggle, through information operations, strategic goals are achieved. The significance of information security as a component of Ukraine's military security is due to the dependence of the implementation of the most important interests of Ukraine in the military sphere from information threats. It was determined that the most significant threat to the national security of Ukraine in the information sphere is the implementation by foreign countries of a negative informational and psychological impact on the public consciousness of Ukrainian citizens and the world community through information campaigns and campaigns, and special information operations. The significance of information security as a component of Ukraine's military security is due to the dependence of the implementation of the most important interests of Ukraine in the military sphere from information threats. From the analysis of the most dangerous threats to the important national interests of Ukraine in the military sphere, it follows that the implementation basis for most of these threats is informational. It is determined that today information struggle becomes one of the important and basic forms of resolving conflicts between states. Effectiveness of timely detection and neutralization of the considered threats to national security in the military sphere essentially depends on the sensitivity and activity of measures to ensure military security at the information level.*

*Keywords:* threat of military security, information sphere, information war, information security.