УДК 351.004
DOI https://doi.org/10.32782/1813-3401.2023.3.32

Лисенко С. О.
доктор юридичних наук, професор,
директор Інституту безпеки,
ПрАТ «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

АСИМЕТРИЧНІ ВІДПОВІДІ, ПСИХОЛОГІЧНІ ОПЕРАЦІЇ (ПСО) ТА ІНФОРМАЦІЙНА ПІДТРИМКА, ЯК СКЛАДОВІ СТРАТЕГІЧНИХ ПРИНЦИПІВ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Стаття присвячена дослідженню асиметричних відповідей, психологічних операцій та інформаційної підтримки, як стратегічних складових управління інформаційною безпекою держави. У ній розглядається, як ці елементи можуть бути використані для протидії складним сучасним загрозам, таким як кібератаки, дезінформація та гібридна війна, які націлені на цифрову та когнітивну сфери. Досліджуючи теоретичні та практичні засади цих стратегій, стаття підкреслює їх важливість для підвищення стійкості та адаптивності систем національної безпеки перед обличчям нових викликів.

Автор зазначає, що асиметричні відповіді пропонують гнучкий підхід до пом'якшення загроз, дозволяючи державам розробляти нетрадиційні контрзаходи, які використовують вразливі місця в стратегіях супротивників. Цей нелінійний підхід надає критичну перевагу у реагуванні на кіберзагрози та психологічні маніпуляції, особливо – коли традиційні захисні механізми є недостатніми. Також підкреслюється, що психологічні операції є життєво важливим інструментом, який використовується для впливу на громадську думку, протидії ворожим наративам і зміцнення колективного духу та єдності суспільства перед обличчям ворожих зусиль з дестабілізації.

У дослідженні розкриваються етичні та правові аспекти, притаманні реалізації психологічних операцій та систем інформаційної підтримки. Хоча ці стратегії можуть значно посилити національну безпеку, вони потребують ретельного регулювання, щоб уникнути порушення громадянських свобод і зберегти довіру суспільства. Тому необхідні етичні рамки і механізми нагляду, щоб збалансувати цілі безпеки з демократичними принципами, гарантуючи, що ці операції слугують суспільним інтересам, поважаючи при цьому права особистості.

На особливу увагу заслуговує роль інформаційної підтримки у сприянні прийняттю рішень у режимі реального часу та реагуванні на загрози. Завдяки ефективному використанню збору, аналізу та розповсюдженню даних, інформаційна підтримка дозволяє своєчасно і точно реагувати на інциденти, пов'язані з безпекою. Ця функція ще більше посилюється завдяки інтеграції передових інформаційних систем і протоколів захисту, таких як шифрування і контроль доступу, для захисту від порушень. У статті підкреслюється важливість цих компонентів для побудови стійкої, надійної інфраструктури інформаційної безпеки, яка відповідає вимогам сучасного безпекового середовища.

Ключові слова: *інформаційна безпека, управління інформаційною безпекою, стратегічні принципи, державне управління, національна безпека, безпека України, інформаційні системи, методи захисту.*

Обґрунтування актуальності обраної теми. Традиційні заходи безпеки часто виявляються недостатніми для протидії сучасним викликам, пов'язаним з кібервійнами, дезінформаційними кампаніями та гібридними тактиками, які використовують вразливості в цифровій та психологічній сферах. У цьому контексті розробка та інтеграція асиметричних відповідей і психологічних операцій у комплексну систему інформаційної безпеки, стала вкрай важливою для національної безпеки.

© Лисенко С. О., 2023

Асиметричні відповіді дозволяють державам гнучко протидіяти загрозам, використовуючи нетрадиційні стратегії, які експлуатують конкретні слабкі місця в тактиці супротивника. Аналогічно, психологічні операції набувають все більшого значення як засіб протидії дезінформації і психологічній війні - тактиці, що дедалі частіше використовується для дестабілізації і маніпулювання громадською думкою. Керуючи наративами та впливаючи на поведінку, психологічні операції слугують потужним інструментом захисту суспільного духу та підтримки національної стабільності.

З огляду на зростаючу залежність від цифрової інфраструктури і поширеність інформаційних загроз, стратегічна інтеграція цих компонентів - адаптованих, оперативних контрзаходів, цілеспрямованих психологічних операцій і надійних систем інформаційної підтримки - є життєво важливою. Ця тема є актуальною, оскільки вона стосується поточних і нагальних потреб національної безпеки, представляючи перспективний підхід, який адаптує традиційні принципи безпеки до вимог цифрового, взаємопов'язаного світу. Вивчаючи ці стратегічні компоненти, дослідження сприяє розробці стійкої та стабільної політики інформаційної безпеки, яка має вирішальне значення для захисту державних інтересів та суспільної довіри.

Метою дослідження є аналіз та обґрунтування ролі асиметричних відповідей, психологічних операцій та інформаційної підтримки як невід'ємних складових стратегічних принципів управління інформаційною безпекою держави.

Аналіз останніх досліджень та публікацій. Науковці та фахівці з безпеки підкреслюють, що традиційні механізми захисту часто не справляються з витонченими кібератаками, дезінформаційними кампаніями та тактиками гібридної війни. Це призвело до зростання інтересу до асиметричних відповідей, психологічних операцій та посилення систем інформаційної підтримки в рамках комплексних стратегій національної безпеки Дана тематика досліджувалася окремими авторами такими авторами, такими як: Гриіцук Р. В., Канкін І. О., Охрімчук В. В., Гончаренко О. М., Єремєєва І.А., Білоусенко О., Саричев Ю.О., Богданович В.Ю., Бабак В. П. Проте, у даній статті автор більш детально акцентує увагу саме на зміст асиметричних відповідей в контексті інформаційної безпеки.

Основний зміст дослідження. Управління інформаційною безпекою є основою підходу держави до захисту своїх інформаційних активів та забезпечення стійкості систем до нових загроз. Таке управління узгоджується зі стратегічними цілями, забезпечуючи захист національних інтересів від ризиків, пов'язаних з кіберзагрозами, шпигунством та дезінформаційними кампаніями. В основі такого управління лежать такі принципи, як підзвітність, прозорість, управління ризиками та стійкість. Ці принципи, своєю чергою, узгоджуються з національною безпекою, створюючи скоординовану структуру, яка залучає всі урядові сектори до створення надійного, безпечного інформаційного середовища. Такий підхід не лише захищає урядові дані, але й зміцнює національну безпеку, оскільки добре захищена інформаційна екосистема зменшує ризики для критичної інфраструктури та довіри суспільства.

Підзвітність в управлінні інформаційною безпекою вимагає чіткого визначення ролей та обов'язків між державними установами. Коли кожне відомство знає свої конкретні обов'язки щодо захисту інформаційних активів, це зменшує прогалини в заходах безпеки та підвищує ефективність реагування. Наприклад, Міністерство оборони може контролювати кібербезпеку військових мереж, тоді як Міністерство інформації керує стратегіями протидії дезінформації, тобто кожен суб’єкт відповідає за свій сектор. Прозорість також має важливе значення, оскільки сприяє зміцненню довіри між зацікавленими сторонами, в тому числі громадськістю та міжнародними союзниками. Загальнодоступні звіти про ініціативи з кібербезпеки можуть продемонструвати прихильність і прогрес у зміцненні державної безпеки, підвищуючи довіру громадськості.

Управління ризиками передбачає виявлення, оцінку та зменшення загроз інформаційним системам, що є фундаментальною основою для проактивної позиції у сфері безпеки. Держава може здійснювати оцінку загроз для критично важливих систем, регулярно оновлюючи ці оцінки для виявлення нових вразливостей. Стійкість забезпечує безперервність операцій, навіть якщо системи піддаються атаці або компрометації. Це має вирішальне значення для підтримки державних функцій і послуг під час кризи, і багато урядів зараз вимагають від усіх відомств планів реагування на інциденти. Наприклад, після кібератаки на систему податкового адміністрування, стійкий план реагування гарантує, що державні послуги залишатимуться доступними.

Уряд відіграє центральну роль у розробці та впровадженні цих принципів. Його керівництво забезпечує дотримання стандартів у всіх секторах і наявність у відомств необхідних ресурсів для забезпечення безпеки. Уряди часто створюють централізовані стратегії кібербезпеки, які стандартизують заходи безпеки в усіх відомствах, що забезпечує уніфіковане реагування [1]. В Україні держава забезпечує інформаційну безпеку через політику, яка вимагає міжвідомчої співпраці, де правоохоронні органи та підрозділи кіберзахисту координують реагування на кіберзагрози. Такий міжвідомчий підхід має вирішальне значення для стійкості, оскільки він гарантує, що навіть при зміні керівництва система безпеки залишається недоторканою.

Інша важлива роль уряду полягає у розподілі ресурсів, наданні необхідних інструментів, навчанні та фінансуванні для забезпечення ефективної інформаційної безпеки. Уряди часто інвестують у навчання персоналу з кібербезпеки, щоб тримати його в курсі останніх загроз і методів захисту. Національна стратегія кібербезпеки України передбачає фінансування розвитку робочої сили, забезпечуючи наявність кваліфікованих кадрів для ефективного управління та експлуатації систем безпеки. Крім того, уряд забезпечує дотримання стандартів безпеки, вимагаючи, щоб установи відповідали визначеним критеріям для підтримання високого рівня безпеки. Коли установи повинні дотримуватися встановлених урядом протоколів шифрування даних і контролю доступу, підтримується єдиний стандарт безпеки.

Урядові установи також співпрацюють з міжнародними партнерами для розробки стандартів, які відповідають глобальним рамкам безпеки, сприяючи співробітництву в галузі кібербезпеки. Транскордонні кіберінциденти вимагають спільного реагування, а угоди з сусідніми країнами уможливлюють взаємну допомогу в розвідці загроз. Співпраця України з Європейським Союзом у сфері кібербезпеки є одним з таких прикладів, що дозволяє обмінюватися ресурсами, розвідданими та швидко реагувати на регіональні загрози. Розвиваючи міжнародні відносини, уряд зміцнює спроможність країни реагувати на інциденти, пов'язані з безпекою, за межами її кордонів, сприяючи створенню більш безпечної глобальної інформаційної екосистеми.

Асиметричні відповіді в інформаційній безпеці передбачають контрзаходи, які навмисно відрізняються від масштабу, технології або безпосереднього характеру початкової загрози [2]. Замість того, щоб копіювати метод або ресурси зловмисника, ці відповіді стратегічно розробляються для використання конкретних вразливостей у підході зловмисника. Ця стратегія особливо корисна, коли держава стикається із загрозами, які використовують нетрадиційні або гібридні тактики, де традиційні засоби захисту можуть бути неефективними. Асиметричні відповіді використовують непередбачуваність і залучають альтернативні ресурси для нейтралізації загроз, часто досягаючи більшого ефекту при менших витратах ресурсів. Такий підхід дозволяє державам гнучко і творчо управляти безпековими ризиками, адаптуючись до постійно мінливого ландшафту загроз.

Дані заходи актуальні у сфері державної безпеки, де загрози можуть надходити з різних джерел, включаючи кіберзлочинців, вороже налаштованих державних суб'єктів або організовані кампанії з дезінформації. Вживаючи непередбачувані та інноваційні контрзаходи, уряди можуть вивести супротивників з рівноваги і знизити ефективність їхніх атак. Такий підхід не є дзеркальним відображенням атаки, а передбачає і руйнує майбутні стратегії зловмисника. Крім того, асиметрія дозволяє використовувати непрямі методи, такі як фінансові санкції або дипломатичний тиск, для нейтралізації загрози.

Асиметричні відповіді в стратегіях національної безпеки включають протидію кіберзагрозам за допомогою нетрадиційних методів, таких як обман і дезінформація проти самих зловмисників. Держава, що зазнала кібератаки, може створити «горщики з медом», або системи приманок, призначені для того, щоб заманити зловмисників і викрити їхні методи та наміри. Ці пастки витрачають ресурси супротивника, водночас надаючи цінну інформацію про його методи. Наприклад, під час хвилі кіберінцидентів державні служби безпеки можуть розгортати фальшиві мережеві вузли, які імітують доступ до конфіденційної інформації. Коли зловмисники атакують ці вузли, вони розкривають свої методи і наміри, що дозволяє командам безпеки підготуватися і реагувати більш ефективно. Такий підхід не лише відволікає атаки, але й підриває довіру супротивника до своїх стратегій.

Замість того, щоб просто спростовувати неправдиві наративи, держава може поширювати цілеспрямовану інформацію, спрямовану на вирішення основних соціальних або

політичних проблем, які експлуатуються дезінформацією. Така проактивна стратегія запобігає поширенню дезінформації, безпосередньо залучаючи населення до точної інформації, яка відповідає їхнім інтересам. Коли з'явилася широко розповсюджена дезінформація про безпеку вакцин проти COVID-19, деякі уряди використовували місцевих впливових осіб для поширення правдивої інформації. Замість того, щоб безпосередньо протидіяти кожній дезінформації, ці впливові особи зосередилися на прозорих і достовірних повідомленнях, зменшуючи вплив неправдивих тверджень.

У сценаріях гібридної війни держави також можуть застосовувати асиметричні відповіді, використовуючи цифрові платформи для залучення міжнародних союзників і світової громадськості [3]. Замість того, щоб покладатися на традиційні військові чи дипломатичні канали, країна, якій загрожує небезпека, може публікувати оновлення подій у режимі реального часу, протидіючи ворожим наративам у глобальному медіа-просторі. Така стратегія не лише протидіє дезінформації, але й формує міжнародну підтримку та легітимність позиції держави, створюючи тиск на супротивника.

Асиметричні відповіді виходять за межі цифрових стратегій і включають економічні та правові контрзаходи, які впливають на супротивника опосередковано. Коли держава стикається з атакою на свої фінансові системи, вона може відреагувати введенням суворих економічних санкцій проти країни нападника або організацій, причетних до злочину [4]. Ці санкції можуть не зупинити атаку безпосередньо, але створити значний стримуючий фактор, впливаючи на економіку та політичне становище супротивника. Ці дії спричиняють довгострокові витрати і тиск, стримуючи подальші атаки, але не вступаючи в пряме кіберпротистояння.

Психологічні операції - це стратегічні зусилля, які використовуються в рамках інформаційної безпеки для впливу на сприйняття, ставлення та поведінку конкретних цільових аудиторій. Основною метою психологічних операцій є створення когнітивних та емоційних реакцій, які підтримують цілі безпеки держави. Ці операції можуть варіюватися від зміцнення довіри громадськості до урядових інституцій до стримування ворожих суб'єктів за допомогою цілеспрямованих повідомлень. Формуючи сприйняття і впливаючи на наратив, психологічні операції мають на меті попередити або пом'якшити потенційні загрози безпеці, які можуть зашкодити національній стабільності або суспільному духу [6]. Цей підхід виходить за рамки фізичного або технічного захисту, зосереджуючись на когнітивній сфері, яка набуває все більшого значення в інформаційній безпеці.

Психологічні операції можуть застосовуватися як в оборонних, так і в наступальних цілях для управління інформаційними потоками і протидії психологічній війні. Як оборонний інструмент, психологічні операції допомагають захистити громадськість від дезінформації та ворожого психологічного впливу. Під час кризи дезінформація може викликати паніку або невдоволення, що послаблює здатність уряду ефективно управляти ситуацією. Щоб протидіяти цьому, держава може поширювати чітку, фактичну інформацію через надійні канали, щоб відновити довіру громадськості та роз'яснити хибні уявлення.

Використання психологічних операцій державою, обмежене етичними та правовими міркуваннями. Ці операції часто балансують на тонкій межі між впливом і маніпулюванням, і вони повинні уникати порушення таких фундаментальних прав, як свобода інформації та особиста недоторканність. Етичні міркування особливо актуальні, коли операції спрямовані на широку громадськість, оскільки дезінформація - навіть із захисними цілями - може підірвати довіру, якщо її буде виявлено. Саме тому багато демократичних урядів обмежують психологічні операції прозорими інформаційними кампаніями, наголошуючи на чесності та достовірності, щоб зберегти довіру громадськості.

З юридичної точки зору, психологічні операції часто підпадають під дію міжнародних і національних норм, які регулюють поведінку у воєнний час, права людини і свободу вираження поглядів. Міжнародні угоди, такі як Женевські конвенції, визначають обмеження на психологічні тактики, які можуть спричинити шкоду або надмірний тиск на цивільне населення. У демократичних країнах національне законодавство може вимагати нагляду за тим, щоб психологічні операції не зазіхали на громадянські свободи і не порушували принципи пропорційності [7]. Це означає, що держави повинні балансувати між необхідністю проведення ефективних психологічних операцій і дотриманням правових стандартів, які захищають права громадян.

У багатьох випадках незалежні органи або парламентські комітети здійснюють нагляд за

цими операціями, щоб забезпечити дотримання етичних і правових стандартів. Це гарантує, що, хоча психологічні операції можуть слугувати потужним оборонним інструментом, вони використовуються відповідально і відповідно до демократичних цінностей, зберігаючи баланс між безпекою та етичним врядуванням. Дотримуючись цих меж, держави можуть ефективно використовувати психологічні операції як частину своєї стратегії інформаційної безпеки, не ставлячи під загрозу довіру і права громадськості, зміцнюючи як безпеку, так і легітимність в очах громадян і міжнародної спільноти.

Інформаційна підтримка в управлінні безпекою - це систематичний збір, аналіз і розповсюдження відповідних даних, які допомагають приймати рішення, пов'язані з безпекою. Ця підтримка надає своєчасну, точну і дієву інформацію, що дозволяє органам державного управління і безпеки передбачати, пом'якшувати і ефективно реагувати на потенційні загрози. Інформаційна підтримка має важливе значення в контексті безпеки, оскільки вона лежить в основі процесів прийняття рішень, дозволяючи органам влади ефективно розподіляти ресурси, швидко реагувати на ризики, що виникають, і займати проактивну позицію щодо нових викликів безпеці [8]. Перетворюючи необроблені дані на структуровану інформацію, інформаційна підтримка дає можливість державним установам орієнтуватися в складному і динамічному середовищі загроз.

Інформаційні системи відіграють вирішальну роль в інтеграції та обробці даних, формуючи основу інформаційної підтримки. Ці системи забезпечують управління даними в режимі реального часу, що дозволяє здійснювати безперервний моніторинг і швидко реагувати на інциденти в міру їх виникнення. Завдяки вдосконаленим алгоритмам та аналітиці даних інформаційні системи аналізують величезні обсяги даних з різних джерел, виявляючи закономірності, аномалії та потенційні ризики, які в іншому випадку можуть залишитися непоміченими. Централізована урядова інформаційна система може консолідувати дані з різних відомств, забезпечуючи єдине бачення загроз національній безпеці. Такий інтегрований підхід підвищує обізнаність про ситуацію, оскільки особи, які приймають рішення, мають доступ до всебічної, актуальної інформації, що підвищує точність і своєчасність рішень у сфері безпеки [9]. Інформаційні системи також підтримують автоматичне оповіщення, негайно повідомляючи персонал служби безпеки про перевищення певних порогових значень або параметрів.

Для підтримки цілісності та конфіденційності цих інформаційних систем застосовуються різні методи захисту від потенційних порушень. Контроль доступу формує першу лінію захисту, гарантуючи, що лише уповноважений персонал має доступ до конфіденційної інформації. Ці засоби включають багатофакторну автентифікацію, протоколи доступу на основі ролей і безпечні процедури входу в систему, які запобігають несанкціонованому доступу і знижують ризик внутрішніх загроз. Для доступу до критично важливих даних співробітники служби безпеки можуть використовувати біометричну ідентифікацію разом із захистом паролем, що створює додатковий рівень безпеки, який обмежує доступ лише для тих, хто має підтверджений допуск.

Шифрування - ще один фундаментальний метод захисту, який кодує дані так, щоб їх могли прочитати лише уповноважені особи [10]. Це гарантує, що навіть якщо дані перехоплені під час передачі, вони залишаються нечитабельними для сторонніх осіб. Шифрування широко використовується в урядових системах, особливо при передачі конфіденційних даних між відомствами або при спілкуванні із зовнішніми партнерами. Наприклад, конфіденційне спілкування між розвідувальними службами може бути зашифроване, щоб запобігти перехопленню ворожими суб'єктами, зберегти конфіденційність інформації та захистити інтереси національної безпеки.

Регулярний моніторинг і аудит ще більше посилюють інформаційну безпеку, виявляючи і усуваючи вразливості в режимі реального часу. Безперервний моніторинг дозволяє командам безпеки виявляти незвичну активність, таку як повторні невдалі спроби входу в систему або несанкціоновану передачу даних, що може свідчити про потенційне порушення. Ці системи моніторингу часто включають автоматизовані механізми сповіщення, які негайно повідомляють адміністраторів про виявлення підозрілої активності, що дозволяє швидко реагувати. Крім того, регулярні аудити допомагають виявляти та виправляти прогалини в системі безпеки, гарантуючи, що захисні заходи системи є актуальними та ефективними. Державна установа може проводити щоквартальні аудити своїх інформаційних систем, переглядаючи

журнали доступу та протоколи безпеки, щоб виявити сфери, які потребують вдосконалення, і забезпечити відповідність оновленим політикам безпеки.

Впроваджуючи ці методи захисту, держави можуть убезпечити свої системи інформаційного забезпечення від зовнішніх загроз і внутрішніх вразливостей. Захист цих систем має вирішальне значення, оскільки порушення може поставити під загрозу не лише конфіденційні дані, але й здатність держави ефективно реагувати на інциденти, пов'язані з безпекою. Таким чином, інформаційне забезпечення, коли воно добре захищене, слугує наріжним каменем управління безпекою, дозволяючи урядам приймати обґрунтовані, своєчасні рішення, які підтримують національну безпеку і довіру суспільства. Поєднання надійної інфраструктури даних і проактивних заходів захисту створює стійке інформаційне середовище, гарантуючи, що критична інформація залишається захищеною і доступною, коли вона найбільше потрібна.

Висновки та перспективи подальших досліджень. Таким чином, інтеграція асиметричних відповідей, психологічних операцій та всебічної інформаційної підтримки, формує багатогранний підхід до управління інформаційною безпекою держави. Ці компоненти разом підвищують стійкість і адаптивність заходів національної безпеки в епоху, коли кіберзагрози, дезінформація і тактика гібридної війни стають все більш поширеними. Асиметричні відповіді дозволяють державам творчо та ефективно протидіяти загрозам, а психологічні операції дозволяють пом'якшити вплив ворожих наративів і значною мірою формувати сприйняття громадськості та супротивника у вигідний для національної безпеки спосіб.

З огляду на делікатний баланс між впливом і маніпуляцією, майбутні дослідження могли б вивчити рамки, які забезпечують проведення цих операцій прозоро і етично, зберігаючи довіру громадськості і водночас – гарантуючи ефективність. Ще одним перспективним напрямком досліджень є розробка передових асиметричних стратегій реагування на основі штучного інтелекту, які використовують машинне навчання для більш ефективного передбачення і протидії кіберзагрозам. Крім того, оскільки інформаційні системи стають дедалі складнішими, дослідження вдосконалених методів захисту – таких як квантове шифрування і вдосконалені алгоритми виявлення аномалій – можуть значно посилити стійкість систем інформаційного забезпечення.

Ці напрямки подальших досліджень не лише відкривають можливості для вдосконалення існуючих стратегій інформаційної безпеки, але й дають уявлення про те, як держави можуть адаптуватися до нових загроз і технологічного прогресу. Продовжуючи розвиватися і впроваджувати інновації в цих сферах, держави можуть зміцнити свою оборону, гарантуючи, що інформаційна безпека залишається основою національної стійкості і суспільної довіри у все більш взаємопов'язаному світі.

Список використаної літератури:

1. Гриіцук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17, № 1. С. 80-86.
2. Гончаренко О. М. Асиметричні стратегії в зовнішній політиці. *Політика і час*. № 12. 2005. С. 50-56.
3. Гончаренко О. М. Концептуальні засади та критерії ефективності асиметричних стратегій в міжнародних відносинах. *Молодий вчений*. 2016. № 4.1 (31.1). С. 45-49.
4. Єремєєва І.А. Проблеми асиметричного конфлікту в сучасних міжнароллних відносинах. *Регіональні студії*. 2018. № 14. С. 87–91.
5. В Україні запустили defense tech cluster BRAVE1, який стимулюватиме розвиток військових інновацій та оборонних технологій. *Офіційний сайт Міністерства цифрової трансформації України.* 2023 р. URL: https://www.kmu.gov.ua/news/v-ukrainizapustyly-defense-tech-cluster-brave1-iakyi-stymuliuvatyme-rozvytok-viiskovykh-innovatsii-taoboronnykh-tekhnolohii/.
6. Білоусенко, О. (2022). Що таке інформаційно-психологічні операції і як їх розпізнати. *ms.detector.media.* URL: https://ms.detector.media/manipulyatsii/post/29009/2022-02-23-shcho-take-informatsiyno-psykhologichni-operatsii-i-yak-ikh-rozpiznaty/
7. FM 3-05.301 Psychological Operations Tactics, Techniques, and Procedures. 2003, dec. URL: https://fas.org/irp/doddir/army/fm3-05-301.pdf
8. Саричев Ю.О. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління. *Вісник НАДУ при Президентові України (Серія "Державне управління")*. 2017. № 3. С. 120-126.
9. Богданович В.Ю. Методика формування та управління інтегрованим потенціалом протидії загрозам воєнного характеру для забезпечення визначеного рівня воєнної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони: Зб. наук. пр. НУОУ ім. Івана Черняховського*. 2018. № 2(32). С. 81-86.
10. Бабак В. П. Теоретичні основи захисту інформації : підручник. *Книжкове видавництво НАУ*, 2008. – 752 с.

Lysenko S. O. Improvement of strategic principles of state management of information security as part of national security of Ukraine

The article is devoted to the study of asymmetric responses, psychological operations, and information support as strategic components in state information security management. It examines how these elements can be leveraged to counteract complex modern threats such as cyber-attacks, misinformation, and hybrid warfare, which target the digital and cognitive domains. By exploring the theoretical and practical foundations of these strategies, the article highlights their importance in enhancing the resilience and adaptability of national security frameworks in the face of evolving challenges.

The author notes that asymmetric responses offer a flexible approach to threat mitigation, allowing states to develop unconventional countermeasures that exploit vulnerabilities in adversaries' strategies. This non-linear approach provides a critical advantage in responding to cyber threats and psychological manipulation, particularly when traditional defense mechanisms are insufficient. Psychological operations are also underscored as a vital tool, used to influence public perception, counter hostile narratives, and strengthen the collective morale and unity of society in the face of adversarial efforts to destabilize.

Revealed in the study are the ethical and legal considerations inherent to the implementation of psychological operations and information support systems. While these strategies can significantly reinforce national security, they require careful regulation to avoid infringing on civil liberties and to maintain public trust. Ethical frameworks and oversight mechanisms are therefore necessary to balance security objectives with democratic principles, ensuring that these operations serve the public interest while respecting individual rights.

Special attention deserves the role of information support in facilitating real-time decision-making and threat response. Through the effective use of data collection, analysis, and dissemination, information support enables timely and accurate responses to security incidents. This function is further enhanced by integrating advanced information systems and protection protocols, such as encryption and access controls, to safeguard against breaches. The article ultimately underscores the importance of these components in building a sustainable, robust information security infrastructure that meets the demands of the modern security environment.

Key words: *information security, information security management, strategic principles, public administration, national security, security of Ukraine, information systems, protection methods.*