УДК: 355.45:004.056(477)

В. В. Мальцев, В. І. Тробюк, І. О. Герасименко

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА СЕКТОРУ ОБОРОНИ УКРАЇНИ

У статті зосереджено увагу на визначенні місця інформаційної безпеки у секторі оборони України, а також на її значенні для захисту суверенітету й демократичних інститутів.

Розглянуто поняття кіберстійкості як спроможності держави, інституцій та громадян протидіяти загрозам і відновлювати функціонування після атак. Проаналізовано досвід створення інтегрованих центрів реагування на інциденти, що поєднують ресурси державного і приватного секторів, забезпечуючи оперативний моніторинг та координацію дій.

Акцентовано на ролі підготовки фахівців із кіберзахисту на міждисциплінарній основ, а також підвищенні рівня медіаграмотності населення, що позитивно впливає на стійкість суспільства до інформаційних впливів.

Інформаційну безпеку в умовах гібридної війни визначено не лише технічним чи організаційним завданням, а й стратегічною складовою оборони держави, яка поєднує політичні, соціальні й технологічні чинники.

***Ключові слова**: інформаційна безпека, гібридна війна, кібероборона, критична інфраструктура, кіберстійкість, медіаграмотність.*

Постановка проблеми. У сучасних умовах повномасштабної збройної агресії проти України проблема забезпечення інформаційної безпеки набула особливої актуальності. Інформаційна безпека вже не сприймається як вузько технологічна сфера – вона стала ключовою стратегічною складовою оборонної політики держави та невід'ємним компонентом національної безпеки.

Сучасні війни характеризуються гібридними методами ведення бойових дій, де поряд із традиційними військовими засобами використовуються кібердиверсії, інформаційно-психологічні операції, пропаганда та дезінформація. У таких умовах перемога неможлива без ефективної протидії цим загрозам, зокрема у кіберпросторі, а також без формування суспільної стійкості до інформаційних впливів. Отже, виникає необхідність переосмислення ролі інформаційної безпеки як системоутворювального чинника ефективного функціонування сектору оборони України з урахуванням як технологічних, так і організаційно-правових аспектів.

Аналіз останніх досліджень і публікацій. Проблематика національної та інформаційної безпеки знайшла своє відображення у наукових працях таких вітчизняних дослідників, як В. Б. Авер'янов, О. Ф. Андрійко, Ю. П. Битяк, В. А. Ліпкан, Н. В. Галіцина, О. В. Голяшкін, Х. П. Ярмак, а також фахівців у сфері кібероборони та кіберстійкості: П. М. Сніцаренка, Ю. М. Саричева, В. А. Гордійчука, В. І. Грицюка та С. А. Запорожця. У працях цих науковців висвітлено адміністративно-правові засади національної безпеки, роль державного регулювання у сфері інформаційної політики, концептуальні засади кібербезпеки як складової захисту інформаційного простору держави, а також підходи до формування кібероборони й розвитку кіберстійкості в умовах гібридної війни.

Однак недостатньо дослідженими залишаються питання інтеграції інформаційної безпеки саме у сектор оборони України, визначення її місця й ролі у загальній архітектурі національної безпеки. Розроблення потребують адміністративно-правові механізми забезпечення інформаційної безпеки у воєнний період і підходи до захисту критичної інформаційної інфраструктури в умовах тривалої гібридної агресії. Це створює підґрунтя для подальшого наукового аналізу й пошуку оптимальних рішень.

Метою статті є аналіз ролі інформаційної безпеки як ключового елемента сектору оборони України в умовах гібридної війни та цифрових загроз, а також її теоретичне обґрунтування. Завдання дослідження полягає у визначенні сучасних технічних, організаційних та адміністративно-правових механізмів забезпечення кіберзахисту в оборонній сфері, виявленні викликів, пов'язаних із захистом критичної інформаційної інфраструктури, а також у формулюванні пропозицій щодо підвищення ефективності національної системи інформаційної безпеки. Окрема увага приділяється вдосконаленню міжвідомчої взаємодії у структурі оборонного сектору України.

Викладення основного матеріалу. У сучасних умовах глобалізації та стрімкого розвитку цифрових технологій питання інформаційної безпеки стало однією з ключових проблем державного

управління і національної безпеки. Україна, перебуваючи в умовах тривалої гібридної війни, стикається з безпрецедентним рівнем кіберзагроз, дезінформаційних кампаній, спроб вплинути на суспільні настрої та порушити функціонування критичної інфраструктури. Інформаційна безпека вже давно перестала бути виключно технічним завданням, а сприймається як стратегічна складова сектору оборони, від ефективності якої залежить стійкість держави в умовах воєнних та інформаційно-психологічних загроз.

Водночас слід зазначити, що сучасні військові конфлікти дедалі більше набувають ознак так званих «війн п'ятого покоління», де вирішальну роль відіграють інформаційно-психологічні операції, кібердиверсії та кампанії впливу на масову свідомість. У таких умовах навіть найрозвиненіше озброєння і класичні оборонні структури можуть виявитися вразливими перед потужними інформаційними ударами. Саме тому інтеграція кібер- та інформаційної безпеки в оборонну архітектуру країни є бажаною і необхідною передумовою національного виживання й розвитку у XXI ст.

Захист інформаційного простору держави вимагає не лише технічних рішень і сучасного обладнання, але й системного підходу до формування відповідної державної політики, створення ефективної нормативно-правового підґрунтя, розвитку людського потенціалу та підвищення суспільної свідомості щодо ризиків інформаційної війни. З кожним роком інформаційні атаки стають дедалі складнішими, спрямовуються на підрив довіри громадян до органів влади, дискредитацію оборонних можливостей країни, маніпулювання суспільною думкою та посилення внутрішньої нестабільності. У таких умовах державі доводиться постійно адаптуватися до нових викликів і створювати механізми швидкого реагування на загрози, які постають у цифровому середовищі.

Особливої уваги потребує узгодженість дій усіх державних органів, залучених до забезпечення інформаційної та кібербезпеки, а також розвиток взаємодії з громадянським суспільством і міжнародними партнерами. Ефективна система інформаційної безпеки має враховувати не лише захист державних інформаційних ресурсів і критичної інфраструктури, а й підвищення інформаційної культури населення, розвиток медіаграмотності та формування здатності протистояти дезінформаційним кампаніям. Сучасні війни дедалі більше переносяться в інформаційно-психологічну площину, і саме тому важко переоцінити важливість безпечного та стійкого інформаційного простору для збереження державного суверенітету й національної ідентичності.

Сьогодні інформаційна безпека визначає не лише рівень обороноздатності країни, а й рівень її політичної стабільності, демократичності та спроможності до сталого розвитку. Це складна багатовимірна категорія, що охоплює питання законодавчого регулювання, технічних рішень, управлінських підходів і формування суспільних цінностей. Тому актуальність дослідження проблем забезпечення інформаційної безпеки зумовлює необхідність удосконалення існуючих механізмів захисту, інтеграції національних зусиль у цій сфері та впровадження найкращих міжнародних практик. Успішність держави у протидії гібридним загрозам безпосередньо залежить від того, наскільки цілісною та ефективною буде побудована система інформаційної безпеки на всіх рівнях – від стратегічного до місцевого.

Інформаційна безпека як складова національної безпеки сьогодні є ключовим пріоритетом державної політики. Стрімке поширення цифрових технологій і перехід багатьох суспільних процесів у кіберпростір поставили державу перед новими викликами й загрозами, що вимагають адекватного правового, організаційного й технічного реагування. В Україні, яка перебуває під постійним тиском гібридної агресії, питання забезпечення безпеки інформаційного простору набуло надзвичайної актуальності, адже від ефективності протидії інформаційно-психологічним і кібернетичним загрозам залежить стабільність внутрішньополітичної ситуації, збереження державного суверенітету й демократичних інститутів.

Інформаційна безпека визначається як захищеність інформаційного середовища держави, суспільства та особи від зовнішніх і внутрішніх загроз, що можуть завдавати шкоди інтересам України. На думку науковців, сучасні виклики мають комплексний характер – вони поєднують кібернетичні атаки, дезінформаційні кампанії, маніпулювання громадською думкою та спроби підриву критичних об'єктів інфраструктури. Розвиток цифрових технологій зумовив виникнення принципово нових загроз: кіберзлочинність набула транснаціонального характеру і здатна завдати значної шкоди інтересам особи, суспільства і держави загалом [4].

Ці загрози неможливо нейтралізувати виключно технічними заходами. Вони потребують системного підходу, а саме: створення нормативно-правового підґрунтя, підготовки кадрів,

упровадження інноваційних технологій, підвищення рівня культури, безпечної поведінки громадян у цифровому середовищі. Дослідники зауважують, що інформаційна безпека є компонентом оборонної політики і важливим чинником демократичного розвитку, оскільки забезпечує публічність і прозорість влади, захищає громадян від маніпуляцій і пропаганди, підтримує високий рівень довіри до державних інститутів [4].

У сучасних умовах інформаційна безпека стала не лише технічним викликом, а й стратегічною складовою обороноздатності. Українська держава зазнає нових кібернетичних, інформаційно-психологічних атак, які агресор спрямовує на підрив довіри до національних інститутів і посилення суспільної напруженості. Протистояння цим загрозам потребує створення ефективної системи кіберзахисту, інтегрованої в оборонну архітектуру держави.

На думку П. М. Сніцаренка, кібероборону слід розглядати не як окрему сферу, а як невід'ємну частину сектору оборони держави з чітко визначеною структурою, складовими та етапами реалізації [1]. Науковець обґрунтував сутність кібероборони, окреслив елементи загальнодержавної системи захисту та взаємозв'язки між ними, що становить важливе підґрунтя нашого дослідження.

Кібероборону необхідно також розглядати як міждисциплінарну сферу, що об'єднує фахівців різних галузей: інформаційні технології, право, соціологія, психологія, військова справа. Лише їхня скоординована робота дасть змогу створити дієву й адаптивну модель реагування на загрози, що постійно змінюються. Успішність таких команд залежить від гнучкості, міжвідомчої взаємодії та спільного стратегічного бачення.

Одним із перспективних напрямів розвитку кібероборони є створення інтегрованих центрів реагування на інциденти, які функціонують на стику оборонного і цивільного секторів. Такі центри у змозі забезпечити цілодобовий моніторинг інформаційного простору, швидко виявляти й локалізувати кібератаки, проводити розслідування інцидентів і координувати дії між відомствами й приватними структурами. Досвід європейських країн і США демонструє, що саме інтеграція державних і недержавних ресурсів під єдиним командуванням забезпечує максимальну ефективність захисту в умовах гібридних загроз [9, 10].

Сучасна модель кібероборони, на думку П. М. Сніцаренка, має охоплювати захист інформаційних ресурсів і запобігання несанкціонованому доступу до них, передбачати активні дії у відповідь на кіберзагрози, що є частиною військово-політичної стратегії держави. Автор наголошує на потребі чіткого нормативного визначення терміна «кібероборона», що уможливить систематизацію функціональних обов'язків суб'єктів національної безпеки й оборони у цифровому просторі, формування міжвідомчого розподілу повноважень і забезпечить координацію дій у межах єдиного державного механізму [5, 1]. Це положення повністю корелює з потребами України в умовах постійної гібридної агресії, коли саме інформаційно-комунікаційний простір став однією з ключових арен протистояння.

На актуальність формування дієвого міжвідомчого механізму кіберзахисту звертає увагу й С. А. Запорожець. У своєму дослідженні він наголошує, що інформаційні впливи й кібератаки в умовах гібридної війни є засобом деморалізації населення, ефективним інструментом дестабілізації оборонного сектору. Отже, формування системи кібербезпеки потребує комплексного підходу – поєднання ресурсів державних структур, збройних формувань, спеціальних служб та громадянського суспільства. Така модель дасть змогу ефективно координувати дії у разі масштабної кібератаки, швидко локалізувати наслідки й відновлювати працездатність критичної інфраструктури [3].

Особливої актуальності набуває поняття кіберстійкості – здатності держави, її інституцій і громадянського суспільства витримувати, адаптуватися й реагувати на кібератаки з мінімальними втратами. У статті П. М. Сніцаренка, Ю. М. Саричева, В. А. Гордійчука та В. І. Грицюка обґрунтовано, що саме розвиток кіберстійкості є ключовим елементом стратегії протидії гібридним загрозам. На їхню думку, стійкість визначається наявністю технічних засобів захисту, кадровою підготовкою, наявністю чітких алгоритмів реагування, міжнародною підтримкою та рівнем довіри громадян до державних інституцій. Автори визнають важливу роль кіберволонтерських об'єднань, які на початку повномасштабної агресії рф значною мірою компенсували слабкість державної системи кібероборони, і наголошують на необхідності інституціоналізації такої співпраці [6].

У межах розбудови секторальної кіберстійкості важливо також акцентувати увагу на освітній складовій. В умовах швидкого розвитку технологій і змін у природі загроз професійна підготовка фахівців із кіберзахисту має враховувати новітні тенденції, бути адаптивною, міждисциплінарною і ґрунтуватись як на теоретичних знаннях, так і на практичних навичках. Освіта у сфері інформаційної

безпеки не має обмежуватися лише вузькотехнічними спеціалізаціями, а охоплювати знання з інформаційної політики, психології, права та менеджменту. Такий підхід уможливить підготовку фахівців, здатних працювати на перетині технологій і національної безпеки, що є критично важливим для оборонного сектору.

Висновки

Узагальнюючи викладене, можна стверджувати, що ефективна модель інформаційної безпеки як складової сектору оборони України має ґрунтуватися на таких ключових принципах:

1) нормативна визначеність і координація дій усіх залучених суб'єктів;

2) розвиток технічної інфраструктури та оперативне реагування;

3) системне навчання й підготовка фахівців;

4) розвиток кіберстійкості, що охоплює як технологічні, так і соціальні чинники.

Успішність держави у протидії сучасним загрозам в інформаційному просторі залежить від здатності інтегрувати ці елементи в єдину державну систему кібероборони. Ураховуючи досвід останніх років, зокрема 2022–2024 рр., коли кібератаки стали невід'ємною частиною воєнних дій, очевидним є те, що побудова сильної системи інформаційної безпеки є не лише стратегічною метою, а питанням виживання держави в умовах гібридної війни.

Наукові пошуки спрямовуватимуться на подальше дослідження загроз телекомунікаційних технологій.

Перелік джерел посилання

1. Сніцаренко П. М. Кібероборона України як складова оборони держави. *Наука і оборона.* 2024. № 4. С. 40–48.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02.08.2025).
3. Запорожець С. А. Стан забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни. *Політологічний вісник*. 2019. № 83. С. 16–25.
4. Коваль Г. В., Кобко Є. В., Кобко В. А. Інформаційна безпека в системі національної безпеки: адміністративно-правовий аспект. *Вісник ХНТУ. Публічне управління та адміністрування*. 2022. № 1 (80). С. 103–108.
5. Сніцаренко П. М. Про сутність кібероборони як виду воєнних дій. *Наука і оборона.* 2024. № 3. С. 45–54.
6. Сніцаренко П. М., Саричев Ю. О., Гордійчук В. В., Грицюк В. В. Кіберстійкість в умовах воєнної агресії РФ: досягнення України та проблемні питання. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2023. № 3. С. 31–38.
7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента від 14.09.2020 р. № 392/2020. URL : https://surl.lt/tvhhyj (дата звернення: 02.08.2025).
8. Про рішення Ради національної безпеки і оборони України від 19 лютого 2021 року «Про стан виконання рішень Ради національної безпеки і оборони України» : Указ Президента України від 26.02.2021 р. № 77/2021. URL: https://zakon.rada.gov.ua/laws/show/77/2021#Text (дата звернення: 02.08.2025).
9. Allies agree new NATO Integrated Cyber Defence Centre. NATO. URL : https://surl.li/dhyhvk (accessed: 2 August 2025) [in English].
10. The National Cyber Incident Response Plan (NCIRP). *Cybersecurity and Infrastructure Security Agency (CISA).* URL : https://surl.lt/noouvk (accessed 2 August 2025) [in English].

Стаття надійшла до редакції 16.08.2025 р.

UDC: 355.45:004.056(477)

V. Maltsev, V. Trobiuk, I. Herasymenko

INFORMATION SECURITY PROVISION IN THE DEFENSE SECTOR OF UKRAINE

Modern warfare increasingly unfolds in the information-psychological domain. Ukraine, facing prolonged hybrid aggression from Russia, confronts large-scale cyberattacks, disinformation campaigns, and attempts to undermine public trust in state institutions and societal unity. In response to these challenges, the role of information security has evolved into a key element of the state's defense policy and a crucial condition for its survival and development.

The article focuses on defining the role of information security within Ukraine's defense sector and its importance for protecting sovereignty and democratic institutions. It outlines the characteristics of current threats, including cyber sabotage targeting critical infrastructure, manipulation of public opinion, and discrediting campaigns against the Armed Forces and government bodies. In this context, traditional weaponry and defense structures remain vulnerable without robust protection of the information space, requiring modern technical solutions and coordinated efforts among all government institutions, civil society, and international partners.

The concept of cyber resilience is examined as the capacity of the state, institutions, and citizens to withstand threats and restore functionality after attacks. The experience of establishing integrated incident response centers, which combine resources from the public and private sectors to provide real-time monitoring and coordinated action, is analyzed. The article highlights the importance of interdisciplinary training for cybersecurity specialists and raising public media literacy, which enhances societal resistance to information influence.

In conclusion, information security amid hybrid warfare is presented not merely as a technical or organizational task but as a strategic component of national defense, encompassing political, social, and technological factors. Building an effective system of information security and cyber defense determines Ukraine's success in countering modern threats and preserving statehood.

***Keywords**: information security, hybrid warfare, cyber defense, critical infrastructure, cyber resilience, media literacy.*

Мальцев Віталій Вікторович – кандидат юридичних наук, старший дослідник, доцент кафедри державної безпеки, Київський інститут Національної гвардії України
https://orcid.org/0009-0003-3520-1152

Тробюк Володимир Іванович – кандидат військових наук, професор, начальник навчально-наукового центру організації освітнього процесу, Національна академія Національної гвардії України
https://orcid.org/0000-0002-3248-2935

Герасименко Ігор Олександрович – здобувач вищої освіти, Київський інститут Національної гвардії України
https://orcid.org/0009-0005-1362-3236