УДК 343.1
DOI https://doi.org/10.32782/app.v76.2025.6

О. В. Селецький
orcid.org/0000-0002-8291-9736
кандидат юридичних наук, доцент,
декан юридичного факультету
Національного університету «Чернігівська політехніка»

Н. О. Крес
orcid.org/0009-0004-2768-6644
студентка ІІ курсу магістратури юридичного факультету
Національного університету «Чернігівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Постановка проблеми. Інформаційна безпека є однією з ключових складових національної безпеки, особливо в умовах воєнного стану, коли держава стикається з багатогранними викликами, які проявляються як у реальному, так і в цифровому середовищі. В умовах сучасної гібридної війни, яку веде російська федерація проти України, інформаційний фронт став не менш важливим за бойові дії на лінії зіткнення. Маніпуляції свідомістю, поширення фейкових новин, спроби зламів державних і критичних інформаційних систем – усе це загрожує не лише стабільності суспільства, а й ефективності військового та політичного управління.

Стрімкий розвиток інформаційно-комунікаційних технологій та формування інформаційного суспільства зумовлюють пріоритетність завдань щодо захисту інформаційного простору та збереження інформаційного суверенітету. Сучасний інформаційний простір перетворився на поле геополітичної боротьби, де кібератаки, дезінформація та маніпулятивні технології активно застосовуються як елементи гібридних стратегій. Це суттєво підвищує значення інформаційної безпеки як ключової складової частини національної безпеки, особливо в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження проблем інформаційної безпеки зробили такі науковці, як І. О. Валюшко, В. І. Гурковський, В. П. Кононенко, Л. І. Мазуренко, О. О. Мислива, А. Ю. Нашинець-Наумова, Д. В. Смотрич та інші.

Мета статті – здійснити комплексний аналіз сутності та ролі інформаційної безпеки в системі національної безпеки України, з'ясувати специфіку її забезпечення в умовах воєнного стану.

Виклад основного матеріалу. Воєнний стан, який передбачає особливий правовий режим, вимагає посилення захисту інформаційного простору як елемента забезпечення державного суверенітету. В умовах постійної кіберзагрози з боку країни-агресора, важливою стає стратегія інформаційної протидії, яка включає не лише технічні засоби, а й інформаційну політику держави, контрпропаганду, забезпечення інформаційної гігієни в суспільстві та медіаграмотності громадян.

Одним із найважливіших завдань держави є протидія дезінформації та ворожій пропаганді. В умовах війни противник активно використовує маніпулятивні технології для створення паніки серед населення, підриву довіри до державних інституцій та дестабілізації українського суспільства. Тому органи державної влади здійснюють оперативне виявлення та нейтралізацію фейкових новин, спростовують ворожі інформаційні атаки, а також ведуть системну комунікацію з громадянами через офіційні канали (Селецький, Костюченко, 2025, С. 102).

Як зазначають Д. Смотрич та Л. Браілко, починаючи з 2014 року, Україна активно протистоїть багатоплановим інформаційним атакам, які набули особливої інтенсивності після повномасштабного вторгнення у 2022 році. Російські операції інформаційного впливу мають на меті деморалізувати населення, дестабілізувати внутрішню політичну ситуацію та підірвати

довіру до Збройних Сил України та органів державної влади. В таких умовах інформаційна безпека повинна охоплювати не лише оборонні заходи, але й активне формування наративу, який відповідає національним інтересам (Смотрич, Браілко, 2023, С. 124).

І. О. Валюшко зауважує, що агресія російської федерації на сході України виявила непідготовленість українського суспільства одразу ж здійснити дієвий спротив агресору, спрямований на відновлення територіальної цілісності держави. Інформаційна сфера виявилася однією з найнезахищеніших в безпековому секторі України, виявивши серйозні прогалини у системі законодавчого забезпечення інформаційного простору. Проте, разом з тим, російське збройне втручання в Україну стало двигуном у напрацюванні відповідного законодавства в інформаційній сфері (Валюшко, 2017, С. 31).

Особливу роль в умовах воєнного стану відіграють кіберпідрозділи, як державні, так і волонтерські, які здійснюють моніторинг кіберпростору, запобігають атакам на інформаційні системи критичної інфраструктури, а також здійснюють кібердари у відповідь. Формування таких структур стало відповіддю на новітні виклики в сфері інформаційної безпеки, де традиційні засоби захисту виявилися недостатніми.

На думку Д. Тініна та О. Мисливої, в умовах бойових дій на території країни інформація стає стратегічним ресурсом. Її збереження, достовірність і контроль над потоками мають безпосередній вплив на хід воєнних операцій. Неправильно подана або вчасно не заблокована ворожа інформація може призвести до втрат на фронті, підриву морального духу або навіть руйнування стратегічних об'єктів. Тому функція інформаційної безпеки включає не лише технічний, а й комунікаційний компонент (Тінін, Мислива, 2023, С. 137).

Одним із головних викликів залишаються соціальні мережі, які використовуються як інструмент психологічного впливу на населення. Через них поширюється паніка, фейки, дезінформація, маніпулятивні меседжі. В умовах воєнного стану держава обмежила доступ до ресурсів, що прямо загрожують національній безпеці (наприклад, на території України неможливо відкрити, переглянути, використовувати більшість російських вебсайтів). Закон України «Про медіа» (Про медіа, 2022) передбачає спеціальні правила для медіа-сфери у період воєнної агресії з боку російської федерації. У зв'язку з цим Національна рада з питань телебачення і радіомовлення розпочала формування переліку аудіовізуальних сервісів на замовлення та платформ-провайдерів, які пов'язані з країною-агресором. До цього переліку включаються сервіси, що зареєстровані у державних реєстрах рф, використовують російську мову як основну, а також керуються законодавством країни-окупанта. Такі ресурси підлягають блокуванню. Рішення про обмеження доступу до вказаних інтернет-ресурсів приймає Національна комісія, яка відповідає за регулювання в галузях електронних комунікацій, поштових послуг та радіочастот. Крім вебсайтів, забороняється також використання мобільних застосунків зазначених сервісів та встановлення їх програмного забезпечення. До списку вже внесено десятки російських платформ, серед яких: Ivi, Tvigle, Premier, Start, More.tv, Okko, 24ТВ тощо. Однак ефективність таких заходів залежить від здатності громадян критично мислити та протистояти інформаційному впливу.

Законодавче забезпечення інформаційної безпеки у період війни було значно оновлено. Було ухвалено ряд змін до законів щодо кіберзахисту, доступу до інформації, відповідальності за поширення фейків. Водночас виникла потреба в балансі між захистом і свободою слова. Використання воєнного стану як підстави для обмеження прав має бути чітко регламентованим, щоб уникнути зловживань (Ковальова, Яковлева, Чорна, 2024, С. 64).

Освіта в сфері інформаційної безпеки, як для державного сектору, так і для широкої громадськості, набуває вирішального значення. Підготовка фахівців, розвиток кіберграмотності, проведення тренінгів і симуляцій на рівні органів влади – усе це сприяє підвищенню стійкості до інформаційного впливу ззовні. Особливої уваги заслуговує підготовка фахівців, які працюють у сфері стратегічних комунікацій.

Роль медіа у воєнний час також змінилася. Вони стали не лише джерелом новин, а й учасниками інформаційного протистояння. Журналістика у таких умовах вимагає не лише професійності, а й відповідальності. Від швидкості й точності подання інформації залежить багато: від психологічного стану населення до прийняття рішень на рівні управління державою.

Міжнародне співробітництво у сфері інформаційної безпеки стало важливим чинником зміцнення обороноздатності України. Підтримка з боку партнерів, спільні кібероперації, обмін досвідом, технологіями і даними суттєво підвищили спроможності України в цій сфері. Інформаційна інтеграція з НАТО і ЄС стала частиною стратегії національної безпеки (Лелет, 2024, С. 102).

В умовах війни важливо також враховувати гуманітарний аспект інформаційної безпеки. Люди, які опинилися під окупацією або в зоні бойових дій, потребують доступу до об'єктивної інформації. Блокування каналів пропаганди та забезпечення мовлення українських ЗМІ на тимчасово окупованих територіях стало важливим інструментом підтримки зв'язку держави зі своїми громадянами. Інформаційна безпека у воєнний час не є ізольованою сферою – вона перетинається з військовою, економічною, політичною, психологічною безпекою. Це вимагає комплексного підходу до управління інформаційними ризиками, де кожна структура державної влади має чітко визначену роль і функції. Скоординована взаємодія між секторами – запорука стійкості всієї системи безпеки (Мазуренко, 2022, С. 54).

Висновки. Таким чином, інформаційна безпека в умовах воєнного стану є не лише реакцією на зовнішні загрози, а й проактивною політикою формування національної ідентичності, довіри до держави та єдності суспільства. Це складова, без якої неможливе повноцінне функціонування державного механізму в умовах гібридної війни. Сильна інформаційна політика – це сильна держава, готова до викликів сучасного світу.

Література

Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. *Історико-політичні студії. 2017. № 2 (8).* С. 30-43.

Ковальова А., Яковлева А., Чорна А. Кримінальна відповідальність за кіберзлочини, вчинені в умовах воєнного стану. *Матеріали II Міжнародної наукової конференції «Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання» (м. Кропивницький, 19 квітня 2024).* С. 63–64.

Лелет Я. Генеза інформаційної безпеки в умовах воєнно-політичного конфлікту. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. № 19. С. 98–104.

Мазуренко Л. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Питання політології»*. 2022. № 42. С. 50–57.

Про медіа: Закон України №2849-IX від 13.12.2022 року. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (Дата звернення 25.09.2025).

Селецький О. В., Костюченко Н. Д. Поняття та зміст інформаційної безпеки як складової національної безпеки. *Науковий вісник Сіверщини. Серія: Право. № 2 (25), 2025.* С. 98-106.

Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. Серія : Право. 2023. № 77. С. 121–127.

Тінін Д., Мислива О. Деякі аспекти інформаційної безпеки українського населення на тимчасово окупованих територіях. *Матеріали І Міжнародної наукової конференції «Теорія модернізації в контексті сучасної світової науки» (м. Полтава, 23 червня 2023).* С. 137–138.

References

Valiushko, I. O. (2017). Informatsiina bezpeka Ukrainy: transformatsiia zakonodavstva pislia rosiiskoho vtorhnennia [Information security of Ukraine: Transformation of legislation after the Russian invasion]. Istoryko-politychni studii, 2(8), 30–43.

Kovalova, A., Yakovleva, A., & Chorna, A. (2024, April 19). Kryminalna vidpovidalnist za kiberzlochyny, vchyneni v umovakh voiennoho stanu [Criminal liability for cybercrimes committed under martial law]. In Proceedings of the 2nd International Scientific Conference "Intellectual Resource of Today: Scientific Tasks, Development and Challenges" (pp. 63–64). Kropyvnytskyi.

Lelet, Ya. (2024). Geneza informatsiinoi bezpeky v umovakh voienno-politychnoho konfliktu [The genesis of information security in the conditions of military-political conflict]. Visnyk Prykarpatskoho Universytetu. Seriia: Politolohiia, (19), 98–104.

Mazurenko, L. (2022). Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy [Information security in the conditions of the Russian-Ukrainian war: Challenges and threats]. Visnyk Kharkivskoho Natsionalnoho Universytetu imeni V. N. Karazina. Seriia: Pytannia politolohii, (42), 50–57.

Pro media: Zakon Ukrainy № 2849-IX vid 13.12.2022 roku [On media: Law of Ukraine No. 2849-IX of December 13, 2022]. (2022). Retrieved September 25, 2025, from https://zakon.rada.gov.ua/laws/show/2849-20#Text

Seletskyi, O. V., & Kostiuchenko, N. D. (2025). Poniattia ta zmist informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky [The concept and content of information security as a component of national security]. Naukovyi visnyk Sivershchyny. Seriia: Pravo, 2(25), 98–106.

Smotrych, D., & Brailko, L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu [Information security under martial law]. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo, (77), 121–127.

Tinin, D., & Myslyva, O. (2023, June 23). Deiaki aspekty informatsiinoi bezpeky ukrainskoho naselennia na tymchasovo okupovanykh terytoriiakh [Some aspects of information security of the Ukrainian population in temporarily occupied territories]. In Proceedings of the 1st International Scientific Conference "Modernization Theory in the Context of Contemporary World Science" (pp. 137–138). Poltava.

Анотація

Селецький О. В., Крес Н. О. **Інформаційна безпека в умовах воєнного стану як складова національної безпеки. –** Стаття.

Стаття присвячена комплексному аналізу інформаційної безпеки як ключової складової національної безпеки України в умовах воєнного стану. Показано, що війна, розв'язана російською федерацією проти України, суттєво змінила уявлення про характер сучасних загроз, у яких інформаційний фронт виступає не менш значущим, ніж бойові дії на полі бою. Наголошено на важливості протидії дезінформації, фейкам, маніпуляціям громадською думкою та кібератакам, які здійснюються з боку країни-агресора з метою деморалізації населення, підриву довіри до державних інституцій і послаблення обороноздатності країни.

Розкрито роль інформаційної політики держави у формуванні стратегії інформаційної протидії, яка поєднує технічні заходи захисту, розвиток контрпропаганди, підвищення медіаграмотності та інформаційної гігієни громадян. Особливу увагу приділено діяльності державних і волонтерських кіберпідрозділів, що здійснюють моніторинг кіберпростору, запобігають атакам на критичну інфраструктуру та беруть участь у проведенні кібероперацій у відповідь. Визначено значення законодавчих ініціатив, спрямованих на вдосконалення кіберзахисту, блокування ворожих інформаційних ресурсів та обмеження діяльності медіаплатформ, пов'язаних із державою-агресором. Підкреслено необхідність дотримання балансу між забезпеченням інформаційної безпеки та гарантіями свободи слова.

Проаналізовано зміну функцій медіа у воєнний період, їх участь в інформаційному протистоянні та вплив на моральний стан суспільства. Обґрунтовано роль освіти, підготовки спеціалістів у сфері стратегічних комунікацій та розвитку медіаграмотності як інструментів підвищення стійкості держави до інформаційних загроз. Розглянуто питання міжнародного співробітництва, інтеграції України до інформаційного простору НАТО та ЄС, що значно посилило можливості протидії інформаційним викликам.

Зроблено висновок, що інформаційна безпека в умовах воєнного стану виходить за межі технічного чи оборонного виміру, перетворюючись на системоутворюючий чинник забезпечення національної безпеки. Вона слугує інструментом формування національної ідентичності, консолідації суспільства, підтримки довіри до держави та зміцнення її спроможності протистояти гібридним загрозам.

Ключові слова: інформаційна безпека, національна безпека, воєнний стан, дезінформація, кіберзагрози.

Summary

Seletskyi O. V., Kres N. O. **Information security under martial law as a component of national security. –** Article.

The article is devoted to a comprehensive analysis of information security as a key component of Ukraine's national security under martial law. It demonstrates that the modern hybrid war launched by the Russian Federation against Ukraine has significantly reshaped the perception of contemporary threats, where the information front has become no less important than conventional military operations. Particular attention is paid to the challenges of countering disinformation, fake news, manipulative influence on public opinion, and cyberattacks carried out by the aggressor state with the aim of demoralizing the population, undermining trust in public institutions, and weakening the country's defense capability.

The role of state information policy in shaping an effective strategy of information resistance is revealed. This strategy combines technical protection measures, the development of counter-propaganda tools, the promotion of media literacy and information hygiene among citizens. Special emphasis is placed on the activities of governmental and volunteer cyber units that monitor cyberspace, prevent attacks on critical infrastructure, and conduct retaliatory cyber operations. The significance of legislative initiatives aimed at strengthening

cyber defense, blocking hostile information resources, and restricting media platforms associated with the aggressor state is highlighted. At the same time, the article underlines the need to maintain a balance between safeguarding information security and ensuring freedom of speech.

The research examines the transformation of media functions in wartime, noting their direct involvement in the information confrontation and their influence on the psychological resilience of society. The importance of education, training of specialists in strategic communications, and the development of media literacy are substantiated as key instruments for strengthening national resistance to external information threats. Furthermore, the article analyzes international cooperation and Ukraine's integration into the NATO and EU information space, which have significantly enhanced the country's capacity to counter information challenges.

It is concluded that information security under martial law goes beyond a purely technical or defensive dimension, becoming a system-forming factor of national security. It serves as an essential tool for shaping national identity, consolidating society, maintaining public trust in state institutions, and reinforcing the state's resilience against hybrid threats.

Key words: information security, national security, martial law, disinformation, cyber threats.

Дата першого надходження рукопису до видання: 25.09.2025
Дата прийнятого до друку рукопису після рецензування: 21.10.2025
Дата публікації: 21.11.2025