УДК 351.88:004.056.5|(477)«2025»(045)
DOI: https://doi.org/10.32631/v.2025.4.13

Сергій Федорович Константінов,
доктор юридичних наук, професор,
Національна академія Служби безпеки України (м. Київ),
навчально-науковий гуманітарний інститут,
кафедра загальноправових дисциплін (професор);
https://orcid.org/0000-0003-1192-2345,
e-mail: kadmnaiau@ukr.net

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННИЙ ПЕРІОД

Статтю присвячено аналізу адміністративно-правових засобів забезпечення інформаційної безпеки держави в умовах воєнного стану, зокрема в контексті сучасної російсько-української війни. Досліджено теоретичні засади інформаційної безпеки, ключові загрози, організаційно-правові механізми та засоби їх реалізації, спрямовані на захист національного інформаційного простору. Узагальнено, що загрози інформаційній безпеці у 2025 році включають дезінформацію, пропаганду, кібератаки, а також внутрішні вразливості, зокрема низьку інформаційну культуру та витоки даних. Особливу увагу приділено новітнім кіберзагрозам, зокрема атакам, що використовують штучний інтелект, методи соціальної інженерії та атаки на ланцюг поставок, які значно ускладнюють захист критичної інфраструктури. Класифіковано засоби забезпечення інформаційної безпеки на адміністративні, правові, технічні та соціальні.

Ключові слова: інформаційна безпека, адміністративно-правові засоби забезпечення інформаційної безпеки держави, інформаційна безпека держави в умовах воєнного стану, гібридні загрози, критична інфраструктура, дезінформація.

Оглядова стаття

Постановка проблеми

У сучасних умовах геополітичних викликів, зокрема в контексті війни між росією та Україною, що триває, проблема забезпечення інформаційної безпеки держави набуває стратегічного значення. Інформаційна безпека розглядається як стан захищеності інформаційного простору, що гарантує захист національних інтересів, суспільної стабільності й обороноздатності.

Адміністративно-правові засоби є комплексом норм, інститутів і процедур, спрямованих на регулювання інформаційних відносин у воєнний період. У таких умовах адміністративно-правове забезпечення інформаційної безпеки має на меті встановлення нормативних,

організаційних і процедурних меж, що забезпечують захист життєво важливих інтересів держави, суспільства та особи.

Актуальність теми також зумовлена ескалацією гібридних загроз, у яких інформаційний компонент інтегрується з військовими діями. Воєнний стан значно посилює вразливість інформаційного середовища, що потребує адаптації правових механізмів для ефективного реагування на нові виклики.

Стан дослідження проблеми

Наукові дослідження у сфері інформаційної безпеки в умовах воєнного стану активно розвиваються в Україні з 2014 року, зокрема з акцентом на теоретичні, правові та практичні аспекти. Ключові праці фокусуються на балансі між захистом держави та правами громадян.

П. Діхтієвський у статті, присвяченій адміністративно-правовим засобам забезпечення прав, аналізує пріоритети держави в період воєнного стану, пропонуючи інтеграцію правових механізмів для посилення безпеки [1]. В. Політанський розглядає адміністративно-правові засади юридичних обов'язків громадян у контексті національної безпеки [2].

Аспекти забезпечення інформаційних прав суспільства з урахуванням захисту держави розкриваються в роботі Д. Смотрича і Л. Браілка, які досліджують теоретичні аспекти інформаційного захисту, технічні загрози та внутрішні й зовнішні джерела ризиків, підкреслюючи необхідність підвищення інформаційної культури як інструменту протидії інформаційним загрозам [3]. Інші дослідження фокусуються на адміністративно-правовому забезпеченні захисту персональних даних громадян у воєнний період, підкреслюючи вразливості цифрового простору [4]. У роботі Л. Чистоклетова і С. Обрембальського розглядаються особливості забезпечення інформаційної безпеки в умовах російсько-української війни [5].

Окремі праці досліджують адміністративно-правові аспекти адаптації до воєнного часу з акцентом на обмеженнях інформаційних прав заради забезпечення безпеки держави. У статті Б. Мельника йдеться про інформаційну безпеку в умовах воєнного стану та підкреслюється роль державного контролю [6].

О. Власюк аналізує інформаційну безпеку як складову національної безпеки, акцентуючи на соціальній безпеці та інформаційних війнах [7]. С. Бєлай та Д. Корнієнко досліджують систему інформаційного захисту як елемент воєнної безпеки, пропонуючи моделі протидії інформаційним загрозам [8]. Л. Харченко та співавтори надають систематизацію понять, таких як інформаційний суверенітет і захист національного інформаційного простору [9]. В. Шатун та О. Гладун

акцентують увагу на еволюції поняття «інформаційна безпека» в контексті гібридних війн [10]. О. Ільницька аналізує пропагандистські впливи росії та надає рекомендації для вдосконалення державної політики [11]. Є. Стрельцов та співавтори розглядають правові межі інформаційної безпеки в оборонній сфері [12]. В. Кононенко, С. Здоровко й А. Корольова досліджують типологію безпеки в контексті НАТО та гібридної війни [13].

Наукові дослідження демонструють еволюцію від теоретичних концепцій до практичних рекомендацій, акцентуючи увагу на адаптації до гібридних загроз. Однак існує прогалина в емпіричних студіях, які б оцінювали ефективність адміністративно-правових механізмів у забезпеченні інформаційної безпеки.

Мета і завдання дослідження

Метою статті є аналіз і систематизація концептуальних засад, наукових підходів та адміністративно-правових засобів забезпечення інформаційної безпеки в умовах воєнного стану України.

Для досягнення поставленої мети необхідно вирішити такі *завдання*: 1) розкрити теоретичні засади інформаційної безпеки; 2) здійснити огляд наукових досліджень; 3) проаналізувати загрози інформаційній безпеці; 4) оцінити організаційно-правові механізми реагування на загрози інформаційній безпеці; 5) проаналізувати засоби забезпечення інформаційної безпеки; 6) визначити роль органів влади у цьому процесі; 7) сформулювати висновки та рекомендації для підвищення ефективності державного управління в досліджуваній сфері.

Виклад основного матеріалу

Інформаційна безпека в умовах воєнного стану є багатогранною категорією, яка охоплює захист інформації від несанкціонованого доступу, маніпуляцій та деструктивного впливу з метою збереження національного суверенітету. Теоретичні засади інформаційної безпеки ґрунтуються на основних принципах конфіденційності, цілісності та доступності інформації (модель CIA – *confidentiality, integrity, availability*), адаптованих до специфіки воєнного конфлікту [3].

У період воєнного стану інформаційна безпека інтегрується в загальну систему національної безпеки, що визначено в Законі України «Про національну безпеку України»[1]. Теоретична основа інформаційної безпеки передбачає застосування системного підходу, згідно з

[1] Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 13.10.2025).

яким інформаційна сфера виступає підсистемою, тісно взаємопов'язаною з військовою, економічною та соціальною сферами. Збереження балансу між конституційними правами людини (ст. 34 Конституції України) та державними інтересами є надзвичайно важливим, оскільки в умовах воєнного стану дозволяється тимчасове обмеження прав і свобод громадян для запобігання загрозам національній безпеці [5].

Концепція «інформаційної війни», що є складовою частиною гібридної агресії, набуває особливої актуальності в контексті української реальності. Доктрина інформаційної безпеки України визначає теоретичні межі цієї концепції, класифікуючи загрози на зовнішні (наприклад, пропаганда) та внутрішні (наприклад, недостатній рівень контролю)[1]. Теоретичний аналіз також передбачає розроблення превентивних заходів, моделювання можливих сценаріїв і оцінювання ризиків.

Концепція «резилієнтності» – здатності системи відновлюватися після атак – доповнює теоретичні засади інформаційної безпеки. Вона передбачає багаторівневий захист, що охоплює як індивідуальні заходи (медіаграмотність), так і державні стратегії (стратегічні комунікації) [4]. Інформаційна безпека передбачає створення сприятливих умов для розвитку інформаційних потреб особи, забезпечення її захисту від загроз і формування інформаційної культури. Водночас воєнна безпека як складова національної безпеки включає захист від інформаційно-психологічних операцій та маніпулювання інформаційним середовищем із метою створення керованого хаосу [3].

Воєнний період значно посилює наявні загрози, перетворюючи інформаційний простір на арену активної конфронтації. Класифікація загроз в інформаційному середовищі ґрунтується на їхніх джерелах, методах реалізації та потенційних наслідках.

Дезінформація та пропаганда як основні інструменти маніпуляції громадською думкою набувають особливої актуальності в умовах воєнного конфлікту. У контексті російсько-української війни фейкові новини активно використовуються з метою деморалізації населення та підриву довіри до органів влади. За даними Центру протидії дезінформації, з 2022 року було зафіксовано тисячі випадків пропаганди, що спрямовані на дестабілізацію ситуації в Україні[2].

---

[1] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 13.10.2025).

[2] Аналітичний звіт «Мережа російського деструктивного інформаційного впливу CopyCop» // Центр протидії дезінформації : сайт. 09.06.2025. URL:

Кіберзагрози, такі як DDoS-атаки, фішинг, а також несанкціоновані втручання у критичну інфраструктуру, становлять безпосередню загрозу національній безпеці. Як приклад можна навести численні атаки на енергосистеми України в період з 2015 по 2022 роки [14]. Соціальні мережі, своєю чергою, активно використовуються для маніпулювання громадською думкою через фейкові акаунти і ботів, що додатково ускладнює ситуацію [5].

Внутрішні загрози в інформаційному середовищі включають напруженість у зонах дислокації Збройних Сил України, провокації, спрямовані на ескалацію конфліктів, фальсифікацію історичних фактів, а також недбалість і некомпетентність персоналу. Зовнішні загрози походять від агресора, зокрема хакерських атак та інформаційно-психологічних операцій, спрямованих на дестабілізацію ситуації у країні. Водночас низький рівень інформаційної культури серед населення значно знижує здатність до критичного осмислення інформації, що ускладнює захист від таких загроз.

У публічно-інформаційній сфері серйозними загрозами є поширення чуток, панічних настроїв та військової дезінформації, а також витік даних про переміщення військ, що може серйозно зашкодити національній безпеці. Утрати, обстріли й інші військові події лише посилюють чутливість до цих загроз. Вразливими є також персональні дані громадян, які можуть підлягати незаконній обробці, що безпосередньо порушує їхні права та свободи.

Організаційно-правові механізми є структурованою системою органів, норм і процедур. В Україні вони ґрунтуються на конституційних принципах та спеціальному законодавстві.

Інституційна складова включає Раду національної безпеки і оборони (далі – РНБО), Державну службу спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ) і Службу безпеки України (далі – СБУ). Рада національної безпеки і оборони координує політику, ухвалюючи рішення щодо нейтралізації загроз, а Центр протидії дезінформації відіграє ключову роль у моніторингу інформаційної ситуації.

Нормативна база включає Конституцію України (статті 32, 34), закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про національну безпеку України» та «Про правовий режим воєнного стану» [3]. Крім того, станом на сьогодні із запровадженням правового режиму воєнного стану застосовуються Указ Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 64/2022 та рішення РНБО «Про нейтралізацію загроз інформаційній безпеці держави» від

https://cpd.gov.ua/reports/analitychnyj-zvit-merezha-rosijskogo-destruktyvnogo-informaczijnogo-vplyvu-corycop/ (дата звернення: 13.10.2025).

18 березня 2022 року. Зміни до законодавства посилили відповідальність за поширення інформації з обмеженим доступом.

Організаційні механізми включають виконавчі органи влади, суди, Національну раду України з питань телебачення і радіомовлення, Департамент кіберполіції Національної поліції України та ДССЗЗІ. Процедури охоплюють моніторинг, блокування ресурсів, технічні заходи (DNS, IP-блокування) та судовий контроль. Механізми також включають переміщення реєстрів за кордон і обмеження доступу до даних.

Міжнародне співробітництво з ЄС і НАТО, а також ратифіковані договори сприяють обміну досвідом і технологіями [5]. Удосконалення механізмів вимагає посилення координації та використання цифрових інструментів для реагування в реальному часі.

Засоби забезпечення інформаційної безпеки в умовах воєнного стану є комплексом інструментів, спрямованих на превенцію, виявлення та нейтралізацію загроз в інформаційному просторі. Вони поділяються на адміністративні, правові, технічні та соціальні, формуючи комплексний підхід, який забезпечує резилієнтність системи національної безпеки. Цей підхід ґрунтується на принципах пропорційності, законності та ефективності з урахуванням специфіки гібридної війни, де інформаційні операції поєднуються з військовими діями. Згідно із Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27 березня 2025 року № 4336-IX засоби забезпечення інформаційної безпеки посилюються для адаптації до воєнних умов, включаючи резервування даних за кордоном та утворення спеціалізованих підрозділів[1].

Розглянемо кожен тип засобів забезпечення інформаційної безпеки з прикладами, механізмами реалізації та їхньої взаємодією.

Адміністративні засоби охоплюють організаційні процедури, призначення відповідальних осіб та координацію діяльності державних органів для оперативного управління інформаційним простором. Вони спрямовані на створення структур, що забезпечують швидке реагування на загрози, особливо в умовах воєнного стану, коли необхідна централізована взаємодія.

Ліцензування медіа та контроль контенту є ключовими інструментами, які дозволяють регулювати поширення інформації. Наприклад,

[1] Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4336-20 (дата звернення: 13.10.2025).

Національна рада України з питань телебачення і радіомовлення здійснює моніторинг та анулювання ліцензій для запобігання пропаганді, як це відбулося з блокуванням російських каналів із 2022 року. Упровадження єдиних комунікаційних платформ, таких як телемарафон «Єдині новини», забезпечує уніфіковану подачу інформації, мінімізуючи дезінформацію та сприяючи суспільній стабільності. Під час воєнного стану адміністративні засоби також включають утворення підрозділів з кіберзахисту в органах влади, призначення керівників з кіберзахисту з погодженням ДССЗЗІ після перевірки СБУ. Це забезпечує адміністративний контроль за реагуванням на інциденти.

Своєю чергою, адміністративні засоби поділяються на захист інформаційних систем та психологічний захист. Захист інформаційних систем включає впровадження технологій DLP (*Data Loss Prevention*) – для запобігання витокам, та SIEM (*Security Information and Event Management*) – для моніторингу подій і радіоелектронного захисту від електронної розвідки. Психологічний захист передбачає протидію інформаційно-психологічним операціям через виховну роботу у Збройних Силах України та освітні програми для населення, координовані Міністерством оборони України та РНБО [3]. Під час дії правового режиму воєнного стану адміністративні заходи доповнюються створенням національної системи реагування на кіберінциденти, де CERT-UA виступає як національний CSIRT (група реагування на інциденти комп'ютерної безпеки) для аналізу та надання рекомендацій, з координацією через Об'єднану групу реагування в Національному координаційному центрі кібербезпеки. Порядок такого реагування визначається Кабінетом Міністрів України, що забезпечує адміністративну гнучкість.

Правові засоби формують нормативну базу для регулювання інформаційних відносин, установлюючи відповідальність і заборони з посиленням у період воєнного стану для пропорційного обмеження прав з метою забезпечення національної безпеки.

Кримінальна відповідальність за поширення дезінформації в Україні залежить від конкретного випадку. Вона може наставати за поширення завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 Кримінального кодексу України), втручання у приватне життя (ст. 182 Кримінального кодексу України), розголошення комерційної чи банківської таємниці (ст. 232 Кримінального кодексу України) тощо[1]. Адміністративна відповідальність за поширення неправдивих чуток,

[1] Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 13.10.2025).

що можуть викликати паніку серед населення, передбачена ст. 173-1 Кодексу України про адміністративні правопорушення[1]. Цивільна відповідальність за шкоду від поширення неправдивої інформації встановлена ст. 277 Цивільного кодексу України, що дозволяє вимагати спростування такої інформації та відповідної компенсації[2]. Судова практика, зокрема Верховний Суд, підтверджує пропорційність обмежень свободи слова відповідно до трискладового тесту Європейського суду з прав людини, забезпечуючи баланс між правами та безпекою[3].

Законодавство також регулює обробку персональних даних, забороняючи несанкціоноване їх поширення, зокрема в межах Закону України «Про захист персональних даних», з посиленням заходів під час дії воєнного стану, а саме через обмеження доступу до інформації з переліку авторизованих систем. Зміни в законодавстві, запроваджені у 2025 році, вводять заборону на використання програмного забезпечення з відкритого переліку, уведеного ДССЗЗІ, для систем із державними ресурсами та критичної інфраструктури[4]. Крім того, правові засоби включають стандартизацію, зокрема стандарти криптографічного і технічного захисту стають обов'язковими із включенням до національних стандартів. Під час дії воєнного стану правові інструменти дозволяють резервувати дані за кордоном та розміщувати системи на хмарних ресурсах поза межами України в порядку, визначеному Кабінетом Міністрів України, для забезпечення стійкості. Це забезпечує правову основу для міжнародної співпраці, наприклад з ЄС у межах Регламенту щодо захисту персональних даних (GDPR), з обов'язковою державною експертизою засобів захисту.

Технічні засоби забезпечення інформаційної безпеки спрямовані на використання інструментів для захисту, виявлення вразливостей

---

1 Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 № 8073-X // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 13.10.2025).

2 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 13.10.2025).

3 Постанова Верховного Суду у складі колегії суддів Другої судової палати Касаційного цивільного суду від 11.10.2023 : справа № 756/10624/21, провадження № 61-1711св23 // ipLex : сайт. URL: https://iplex.com.ua/doc.php?regnum=114187195&red=100003243c9ef623e5a7ad6aab54b970745657&d=5 (дата звернення: 13.10.2025).

4 Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4336-20 (дата звернення: 13.10.2025).

та резервування даних, що адаптовані до умов воєнного часу, з метою мінімізації наслідків атак на критичну інформаційну інфраструктуру.

Кіберзахист охоплює такі аспекти, як шифрування даних, моніторинг мереж та виявлення несанкціонованого доступу. Державна служба спеціального зв'язку та захисту інформації України здійснює впровадження систем захисту інформації, зокрема комплексного технічного захисту з атестацією для обробки таємної інформації, використовуючи засоби, що мають позитивний експертний висновок. Механізми захисту включають застосування антивірусних програм, двофакторної аутентифікації (2FA) та верифікованого доступу, що є обов'язковими для систем, які обробляють державну інформацію. У період воєнного стану технічні засоби захисту включають створення зашифрованих резервних копій на фізичних носіях для їх зберігання за кордоном, а також заборону на розміщення систем на тимчасово окупованих територіях. Крім того, передбачена регулярна оцінка стану кіберзахисту об'єктів критичної інфраструктури з метою виявлення та усунення вразливостей.

Державний центр кіберзахисту ДССЗЗІ забезпечує функціонування систем захищеного доступу, резервування даних, антивірусного захисту та реагування на кіберінциденти. Технічні стандарти, зокрема базовий профіль безпеки, встановлюються Кабінетом Міністрів України, з подальшою розробкою спеціалізованих профілів для окремих галузей. Процес авторизації систем безпеки здійснюється на декларативній основі, із підтвердженням відповідності вимогам на всіх етапах життєвого циклу системи, включаючи перевірку технічних каналів витоку інформації. Прикладом таких систем є використання технологій SIEM – для моніторингу подій у реальному часі та DLP – для запобігання витокам даних, що інтегруються з національною системою обміну інформацією про кіберзагрози. Такий підхід сприяє забезпеченню технічної резилієнтності національних інформаційних систем, доповнюючи методичні рекомендації ДССЗЗІ, що надаються органам державної влади для ефективного виконання вимог кібербезпеки.

Соціальні засоби спрямовані на підвищення обізнаності громадян та формування культури безпеки, що є важливим превентивним елементом у боротьбі з інформаційними загрозами.

Програми медіаграмотності, координовані Міністерством культури та інформаційної політики України, включають освітні кампанії у школах та онлайн-курси, орієнтовані на розвиток навичок розпізнавання фейкових новин. Однією з таких ініціатив є кампанія «Як не стати овочем» від платформи StopFake. Кампанії протидії пропаганді, зокрема «Інформаційний фронт» від Центру протидії дезінформації,

активно використовують соціальні мережі для спростування дезінформації та поширення правдивих наративів. Стратегічні комунікації влади, зокрема публічні виступи Президента України та звіти урядових органів, сприяють формуванню суспільної єдності і підвищенню довіри до офіційних джерел інформації [5].

Роль ІТ-сектору в умовах воєнного часу також є важливою: впровадження технологій, таких як Starlink, для забезпечення зв'язку в зонах бойових дій, підтримує стабільність комунікацій та доступ до критично важливої інформації. У період воєнного стану соціальні засоби включають навчання персоналу органів державної влади з питань кіберзахисту та підвищення інформаційної культури серед населення, що відповідає рекомендаціям, викладеним у Доктрині інформаційної безпеки України. Інтеграція з міжнародними партнерами, зокрема з НАТО, передбачає обмін досвідом у сфері медіаосвіти та розвитку інструментів боротьби з дезінформацією. Ці соціальні заходи доповнюють інші інструменти інформаційної безпеки, формуючи суспільну резилієнтність через волонтерські ініціативи та діяльність неурядових організацій, таких як Інтерньюз-Україна[1].

Інтеграція адміністративних, правових, технічних і соціальних засобів забезпечує резилієнтність національної системи безпеки з акцентом на превенцію, виявлення та оперативну реакцію на загрози. Наприклад, національна система реагування на кіберінциденти поєднує CSIRT із правовими заборонами і технічним моніторингом, доповнюючи їх соціальними кампаніями для підвищення обізнаності громадян. Захист персональних даних є ключовим для виконання міжнародних зобов'язань, зокрема в контексті Регламенту ЄС щодо захисту персональних даних, і вимагає переоцінки впливу передачі даних в Україну з урахуванням актуальних геополітичних та безпекових ризиків.

Перспективи розвитку включають удосконалення національного законодавства, що має на меті посилення кіберзахисту в умовах війни, з фокусом на застосування технологій штучного інтелекту для аналізу загроз та на розвиток міжнародної співпраці у сфері кібербезпеки. Ефективність цих засобів залежить від належної координації між РНБО та ДССЗЗІ, а також від регулярного проведення аудитів та оцінки поточного стану безпеки для адаптації до змінюваних кіберзагроз.

---

[1] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 13.10.2025).

Висновки

Адміністративно-правові засоби забезпечення інформаційної безпеки в умовах воєнного стану є невід'ємною складовою національної оборони, яка інтегрує теоретичні основи, організаційні механізми та практичні інструменти для протидії гібридним загрозам. Теоретичні засади, засновані на принципах системності, балансу прав і інтересів, підкреслюють важливість забезпечення резилієнтності інформаційного простору, що визначено в Доктрині інформаційної безпеки України. Загрози, такі як дезінформація, пропаганда та кібератаки, вимагають оперативної реакції з акцентом на превентивні заходи, оскільки затримка в реагуванні може призвести до дестабілізації суспільства та підриву обороноздатності, як це спостерігалося під час атак на критичну інфраструктуру з 2015 року.

Організаційно-правові механізми, що включають роль РНБО, ДССЗЗІ та СБУ, потребують подальшого вдосконалення через посилення координації та інтеграції з міжнародними партнерами, зокрема з ЄС та НАТО, для обміну технологіями і стандартами, що дозволить підвищити ефективність на 20–30 % відповідно до глобальних оцінок. Засоби забезпечення – адміністративні (контроль контенту), правові (відповідальність за дезінформацію), технічні (кіберзахист і резервування), соціальні (медіаграмотність) – повинні застосовуватись комплексно з фокусом на інтеграцію як у національній системі реагування на інциденти, що дозволить скоротити час реакції з кількох днів до кількох годин.

Україна має розвинену нормативну базу, проте існує необхідність у посиленні практичної імплементації через регулярні аудити, навчання персоналу, бюджетне фінансування та моніторинг ефективності для адаптації до нових загроз, таких як вплив штучного інтелекту і атаки на ланцюг поставок (*supply chain attacks*), які прогнозуються як ключові у 2025 році. Загалом без системного впровадження цих елементів ризики дестабілізації зростатимуть, тому пріоритетом має стати створення єдиної стратегії з чіткими ключовими показниками ефективності для оцінки прогресу до 2026 року.

У зв'язку із цим необхідно: ухвалити спеціальний закон про інформаційну безпеку в умовах війни; створити єдиний центр протидії дезінформації для координації зусиль; розвивати співпрацю з ЄС і НАТО для обміну технологіями кіберзахисту; проводити регулярні навчання з медіаграмотності для населення; впровадити незалежні аудити для моніторингу ефективності засобів; створити спеціалізовані підрозділи для захисту персональних даних; розробити інформаційні реєстри для військового персоналу з багаторівневим доступом.

Список бібліографічних посилань: 1. Діхтієвський П. В. Адміністративно-правові засоби забезпечення права громадян на особисту

недоторканність в період режиму воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2022. № 6. DOI: https://doi.org/10.54929/2786-5746-2022-6-01-13. **2.** Політанський В. С. Адміністративно-правові засади юридичного обов'язку громадянина в контексті забезпечення національної безпеки у публічно-інформаційній сфері. *Юридичний науковий електронний журнал.* 2025. № 3. С. 643–650. DOI: https://doi.org/10.32782/2524-0374/2025-3/156. **3.** Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77, ч. 2. С. 121–127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20. **4.** Діхтієвський П. В. Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2023. № 10. DOI: https://doi.org/10.54929/2786-5746-2023-10-01-15. **5.** Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії.* 2024. Вип. 31. DOI: https://doi.org/10.5281/zenodo.11381101. **6.** Мельник Б. О. Забезпечення інформаційної безпеки як складова системи національної безпеки України: адміністративно-правові аспекти адаптації до умов воєнного часу // Системний підхід до подолання сучасних викликів крізь призму безпеки, прав людини та права : зб. матеріалів наук.-практ. конф. (м. Вінниця, 12 трав. 2025 р.) / ГО «Молодіжна Організація Починаючих Лідерів». Вінниця, 2025. С. 201–207. **7.** Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : вибр. наук. пр. Київ : НІСД, 2016. 320 с. **8.** Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки // Актуальні проблеми управління інформаційною безпекою держави : зб. тез. наук. доп. IX Всеукр. наук.-практ. конф. (м. Київ, 30 берез. 2018 р.) / МОН України ; М-во інформац. політики України ; Нац. акад. Служби безпеки України. Київ, 2018. С. 12–14. **9.** Інформаційна безпека України: глосарій / Л. С. Харченко та ін. ; за заг. ред. Р. А. Калюжного. Київ : Текст, 2004. 135 с. **10.** Шатун В. Т., Гладун О. В. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія: Державне управління.* 2016. Т. 267, вип. 255. С. 174–180. **11.** Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Гуманітарні візії.* 2016. Вип. 2, № 1. С. 27–32. **12.** Правові основи воєнної безпеки України : монографія / Є. Л. Стрельцов, С. Т. Полторак, Ю. В. Аллеров та ін. ; відп. ред. Є. Л. Стрельцов. Львів : Національна академія сухопутних військ ім. гетьмана Петра Сагайдачного, 2016. 188 с. **13.** Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Т. 2, № 76. С. 244–250.

DOI: https://doi.org/10.24144/2307-3322.2022.76.2.39. **14.** Фесенко О. Д., Колтовсков Д. Г., Остапчук В. М., Макаренко О. О. Аналіз динаміки кібератак на об'єкти критичної інфраструктури в умовах геополітичної напруженості. *Системи і технології зв'язку, інформатизації та кібербезпеки.* 2025. Вип. 7. С. 187–201. DOI: https://doi.org/10.58254/viti.7.2025.17.187.

Надійшла до редколегії 15.10.2025

Прийнята до опублікування 29.11.2025

Konstantinov S. F. Administrative and Legal Means of Ensuring State Information Security in Wartime

This article is devoted to the analysis of administrative and legal means of ensuring state information security in a state of martial law, particularly in the context of the current Russian-Ukrainian war. It examines the theoretical foundations of information security, key threats, organisational and legal mechanisms and means of their implementation aimed at protecting the national information space.

It is noted that the relevance of the topic is due to the escalation of hybrid threats, where the information component plays a decisive role in ensuring national security and social stability. The theoretical foundations are based on the principles of confidentiality, integrity and availability of information (CIA model), adapted to wartime conditions, with integration into the national security system in accordance with the Law of Ukraine "On National Security of Ukraine".

The concepts of information warfare and resilience are considered, which include multilevel protection – from the individual to the state level. A review of scientific research demonstrates the evolution of approaches from theoretical concepts to practical recommendations.

It is stated that threats to information security in 2025 include disinformation, propaganda, cyberattacks (DDoS, phishing, interference with critical infrastructure), as well as internal vulnerabilities such as low information culture and data leaks. Particular attention is paid to the latest cyber threats, including attacks using artificial intelligence, social engineering, and attacks on supply chains, which complicate the protection of critical infrastructure.

It is emphasised that organisational and legal mechanisms cover the activities of the National Security and Defence Council of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, as well as the regulatory and legal framework, including the Constitution of Ukraine, the relevant regulatory and legal framework, and the Decree of the President of Ukraine "On the Introduction of Martial Law in Ukraine" dated 24 February 2022 No. 64/2022. Measures are divided into administrative (media licensing, telethon), legal (criminal and administrative liability), technical (cyber protection, encryption, data backup) and social (media literacy, strategic communications). The Law of Ukraine "On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure" dated 27 March 2025 No. 4336-IX strengthens protection through standardisation and the creation of a national cyber incident response system.

It is concluded that administrative and legal measures are a key element of national defence, but need to be improved through enhanced coordination, practical implementation and international cooperation with the EU and NATO. Relevant recommendations have been made, namely: the adoption of a special law, the creation of a single centre to counter disinformation, the development of cyber technologies, the conduct of regular media literacy training for the population, and the introduction of effectiveness audits. The need for a comprehensive approach to ensure the resilience of the information space by 2026 was emphasised, given the predicted growth of threats from artificial intelligence and cyberattacks.

Keywords: information security, administrative and legal means of ensuring state information security, state information security in conditions of martial law, hybrid threats, critical infrastructure, disinformation.