УДК 342.9:351.746:007:07.1]:355.01(470:477)
DOI https://doi.org/10.32782/2709-3093/2026.5/46

Рожнятівська Н.В.
https://orcid.org/0009-0005-8613-779X
Київський національний університет імені Тараса Шевченка

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СПІВВІДНОШЕННЯ ВІДКРИТОСТІ ТА РЕЖИМУ ТИШІ (2014–2026)

У статті проаналізовано нормативно-правове забезпечення інформаційної безпеки України як безпосередній регулятор комунікаційної взаємодії Збройних Сил України з медіа, що розгортається на перетині між інформаційною відкритістю та режимом тиші. Правовий механізм балансування відкритості й обмеження схарактеризовано як багаторівневу систему, що охоплює конституційний, законодавчий, стратегічно-доктринальний, спеціальний (воєнного стану) і тактично-відомчий рівні регулювання. Показано, що правовий режим доступу до інформації про перебіг бойових дій визначає повсякденні умови роботи медіа в зоні бойових дій: порядок акредитації журналістів, зони доступу, межі висвітлення руху й розташування військ, формати офіційної комунікації сектору безпеки й оборони. Основну увагу приділено еволюції нормативної бази та практик медіавзаємодії за трьома періодами збройного протистояння – антитерористичної операції (2014–2018), операції Об'єднаних сил (2018–2022) та повномасштабного вторгнення і воєнного стану (2022–2026). Установлено, що баланс послідовно зміщувався від переважання відкритості до безпекового обмеження, однак у межах воєнного стану ця динаміка не була лінійною: пікове звуження відкритості 2022–2023 років змінилося частковою лібералізацією 2024–2025 років, досягнутою через інституціоналізований діалог командування з медіаспільнотою. Виявлено суперечність між презумпцією відкритості публічної інформації та безпековою логікою превентивного обмеження, а також юридичну невизначеність режиму тиші, який застосовується як усталений інструмент, проте не має легального визначення, що знижує правову передбачуваність для всіх учасників комунікаційної взаємодії. Запропоновано напрями вдосконалення: легальне закріплення режиму тиші як строкового, обмеженого за обсягом і підконтрольного інструмента; послідовне підпорядкування будь-яких інформаційних обмежень критерію пропорційності; розвиток інституту стратегічних комунікацій, який запобігає утворенню інформаційного вакууму; гармонізація національного регулювання з європейськими стандартами свободи вираження поглядів і доктринами стратегічних комунікацій НАТО.

Ключові слова: *інформаційна безпека, стратегічні комунікації, комунікаційна взаємодія з медіа, інформаційна відкритість, операційна безпека (OPSEC), режим тиші, акредитація журналістів, воєнний стан.*

Постановка проблеми. Інформаційна безпека перетворилася на одну з визначальних умов існування сучасної держави, а її забезпечення давно вийшло за межі суто технічного захисту даних. Сьогодні вона охоплює і протидію деструктивному інформаційному впливу, і збереження інформаційного суверенітету, і водночас гарантування права кожного на доступ до інформації. Саме поєднання цих складників породжує внутрішню суперечність: інформаційна безпека одночасно вимагає відкритості (як умови довіри, підзвітності та стійкості суспільства до маніпуляцій) і обмеження (як засобу захисту чутливих відомостей та протидії ворожому використанню інформації).

Ця суперечність набуває характеру правової проблеми тоді, коли постає питання про межі допустимого обмеження свободи інформації в інтересах безпеки. У мирний період такі межі визначаються переважно галузевим інформаційним законодавством, що виходить із пріоритету відкритості. Натомість в умовах збройної агресії та воєнного стану на перший план виходить безпекова

© Рожнятівська Н.В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

логіка, у межах якої формується практика так званого режиму тиші – тимчасового утримання від оприлюднення певних відомостей. Проблема полягає в тому, що цей інструмент, попри широке застосування, не має сталого легального оформлення, а отже, його співвідношення з конституційним правом на інформацію залишається юридично невизначеним.

Для журналістики ця проблема має цілком практичний вимір: саме правовий режим доступу до інформації про перебіг бойових дій визначає повсякденні умови роботи медіа в зоні бойових дій – від порядку акредитації та кола відомостей, які дозволено оприлюднювати, до відповідальності за передчасне висвітлення перебігу операцій й розташування військ. Відтак нормативна база інформаційної безпеки є не зовнішнім тлом, а безпосереднім регулятором комунікаційної взаємодії Збройних Сил України з медіа, і зміни в ній прямо позначаються на практиках воєнної журналістики та стратегічних комунікацій.

Об'єктом дослідження є нормативно-правове забезпечення інформаційної безпеки України. Предметом дослідження є співвідношення інформаційної відкритості та режиму тиші в цьому забезпеченні, розглянуте крізь призму комунікаційної взаємодії Збройних Сил України з медіа у 2014–2026 роках.

Аналіз останніх досліджень і публікацій. Найближчим до предмета цієї статті є напрям досліджень стратегічних комунікацій, воєнної журналістики та медіаправа, у якому аналізуються взаємодія органів сектору безпеки й оборони з медіа, робота прес-офіцерів і прес-центрів, порядок акредитації та безпеки журналістів у зоні бойових дій, а також стандарти висвітлення російсько-української війни й протидія маніпулятивному контенту. Теоретичне підґрунтя розуміння інформаційного протиборства та гібридної війни закладають праці Г. Почепцова [13] і колективна монографія за редакцією В. Горбуліна [46]. Категоріальний апарат стратегічних комунікацій систематизовано у словнику Т. Попової та В. Ліпкана [10], а інституційне становлення стратегічних комунікацій за стандартами НАТО дослідила А. Баровська [1]. Розвиток стратегічних комунікацій сил оборони в умовах російсько-української війни аналізує І. Іжутова [6], а законодавчі норми та професійні стандарти журналістики воєнного часу – Г. Гребньов [2]. Дедалі більшої ваги набувають праці з кібербезпеки, що розширюють розуміння інформаційної безпеки за рахунок захисту інформаційної інфраструктури [39]. Помітним є й вплив європейських стандартів свободи вираження поглядів, передусім практики застосування статті 10 Конвенції про захист прав людини і основоположних свобод із її вимогою пропорційності обмежень [7].

Водночас бракує праць, у яких відкритість і режим тиші були б осмислені саме як парні, взаємозумовлені елементи єдиного правового механізму інформаційної безпеки, а нормативна база – простежена в її еволюції за періодами збройного протистояння. Здебільшого ці явища розглядаються окремо: відкритість – у контексті прав людини, а обмеження – у контексті безпеки, поза їхньою історико-правовою динамікою. Подолання такої роз'єднаності й систематизація різнорівневих та різночасових правових джерел, що опосередковують баланс відкритості та обмеження, становлять дослідницьку прогалину, на заповнення якої спрямована ця стаття.

Постановка завдання. Метою статті є розкрити структуру й зміст нормативно-правового забезпечення інформаційної безпеки та визначити правовий механізм, що опосередковує співвідношення інформаційної відкритості й режиму тиші, а також простежити еволюцію цього забезпечення за трьома періодами збройного протистояння. Для її досягнення поставлено такі завдання: з'ясувати поняття інформаційної безпеки як об'єкта правового регулювання та її місце в системі національної безпеки; розкрити понятійне співвідношення відкритості, операційної безпеки й режиму тиші в межах моделі «тріади комунікації»; систематизувати правові джерела за рівнями регулювання (конституційний, законодавчий, стратегічно-доктринальний, спеціальний і тактично-відомчий); реконструювати нормативну базу періодів антитерористичної операції (2014–2018), операції Об'єднаних сил (2018–2022) та повномасштабного вторгнення і воєнного стану (2022–2026); зіставити національне регулювання з європейськими та євроатлантичними стандартами; виявити колізії й прогалини та запропонувати шляхи вдосконалення.

Виклад основного матеріалу. У правовому розумінні інформаційна безпека є складним, дворівневим об'єктом. З одного боку, вона захищає інформаційні права особи – право вільно одержувати й поширювати інформацію, право на достовірну інформацію, право на захист персональних даних (стаття 34 Конституції України [8], закон України «Про інформацію» [34] та «Про доступ до публічної інформації» [20]). З іншого – вона захищає суспільство й державу від інформаційних загроз: дезінформації, ворожих інформаційно-психологічних операцій, витоку відомостей, що

загрожують обороноздатності (стаття 17 Конституції України [8], закон України «Про національну безпеку України» [36] та «Про державну таємницю» [19]). Ці два рівні не завжди узгоджуються: те, що зміцнює інформаційні права особи, не завжди зміцнює безпеку держави, і навпаки. Саме тому правове забезпечення інформаційної безпеки не зводиться до простого «захисту», а потребує балансування різноспрямованих інтересів.

Інформаційна відкритість у контексті інформаційної безпеки постає не як абсолютна цінність, а як презумпція: відомості вважаються доступними, доки не доведено правомірність їх обмеження. Відкритість виконує безпекову функцію – вона підтримує суспільну довіру, забезпечує підзвітність влади та підвищує стійкість суспільства до маніпуляцій, оскільки прогалини в офіційній комунікації зазвичай заповнюються дезінформацією.

Протилежним началом у сфері військової комунікації є операційна безпека (OPSEC). OPSEC – це комплекс заходів захисту критично важливих відомостей про плани, дислокацію, чисельність та оснащення підрозділів, розголошення яких може надати перевагу противникові або поставити під загрозу життя військовослужбовців; таке розуміння спирається на доктринальні визначення операційної безпеки у Глосарії термінів і визначень НАТО AAP-06 [47] та в американській доктрині операційної безпеки Joint Publication 3-13.3 [49]. На перетині відкритості й операційної безпеки формується третій складник – публічний імідж інституції, що в умовах війни перетворюється з питання репутації на об'єкт національної безпеки. У прикладних дослідженнях військових стратегічних комунікацій, що спираються на доктринальні підходи НАТО [46; 48], ці три категорії доцільно розглядати як «тріаду комунікації», що перебуває в стані динамічної рівноваги: надмірна відкритість шкодить безпеці, надмірна закритість руйнує довіру та імідж, а імідж є інтегральним показником досягнутого балансу. Саме ця оптика становить концептуальне тло цієї статті й дисертаційного дослідження, до якого вона дотична.

Режим тиші є правовим і практичним інструментом, через який вимога операційної безпеки реалізується у сфері публічної комунікації. Його доцільно розуміти як тимчасове, цілеспрямоване й обмежене за обсягом утримання від оприлюднення певних відомостей до зникнення підстав для обмеження або до їх офіційного підтвердження.

Принципово відмежувати режим тиші від суміжних явищ: від державної таємниці (яка має формалізований і тривалий характер) та від безпідставного замовчування (яке не має легітимної мети й суперечить праву на інформацію). Отже, відкритість і режим тиші не є взаємовиключними: вони утворюють єдину шкалу, на якій правомірне обмеження є вузьким, обґрунтованим винятком із загального правила доступності.

Конституційний рівень регулювання утворюють насамперед статті 17 і 34 Конституції України [8]. Стаття 17 відносить забезпечення інформаційної безпеки до найважливіших функцій держави, надаючи їй найвищого, конституційного статусу. Стаття 34 гарантує свободу інформації й водночас визначає вичерпний перелік легітимних підстав її обмеження – інтереси національної безпеки, територіальної цілісності, громадського порядку, а також захист репутації, прав інших осіб і запобігання розголошенню конфіденційної інформації.

На законодавчому рівні баланс конкретизується двома різноспрямованими масивами норм. Перший – галузеве інформаційне законодавство. Закон України «Про інформацію» закладає загальні засади обігу інформації [34], а Закон України «Про доступ до публічної інформації» закріплює презумпцію відкритості та встановлює трискладовий тест як головний інструмент перевірки правомірності обмеження [20]; на відомчому рівні порядок доступу конкретизує Інструкція із забезпечення доступу до публічної інформації в Міністерстві оборони України та Збройних Силах України [24]. За цією інструкцією доступ може бути обмежено лише тоді, коли обмеження відповідає легітимній меті, його розголошення здатне завдати істотної шкоди, і ця шкода переважає суспільний інтерес в оприлюдненні. Закон України «Про медіа» доповнює цей масив регулюванням діяльності суб'єктів у сфері медіа, зокрема в умовах протидії деструктивному впливу [35].

Другий масив – безпекове законодавство. Закон України «Про державну таємницю» встановлює найвищий рівень захисту відомостей, формалізуючи їх через Звід відомостей, що становлять державну таємницю [19]; тут діє вже зворотна презумпція – обмеження. Закон України «Про основні засади забезпечення кібербезпеки України» поширює захист на інформаційну інфраструктуру, що є невід'ємною складовою інформаційної безпеки [39]. Закон України «Про національну безпеку України» інтегрує ці елементи в єдину систему [36]. До цього ж масиву належить Закон України «Про правовий режим воєнного стану» [41]: серед заходів правового режиму воєнного стану він передбачає, зокрема, можливість заборони передачі

інформації через комп'ютерні мережі (пункт 11 статті 8) та запровадження військовим командуванням додаткових заходів охорони державної таємниці (пункт 22 статті 8). Унаслідок цього в законодавстві співіснують дві логіки: галузева, що виходить із відкритості й індивідуального балансування, та безпекова, що тяжіє до категоризації й обмеження. Узгодження цих логік за критерієм пропорційності й становить основу правового забезпечення інформаційної безпеки.

Стратегічно-доктринальний рівень формують акти політико-правового програмування. Стратегія інформаційної безпеки, затверджена указом Президента України, визначає актуальні загрози, цілі та пріоритети державної політики в інформаційній сфері, серед яких – протидія дезінформації, зміцнення інформаційного суверенітету та розвиток стратегічних комунікацій [43]. Її попередницею була Доктрина інформаційної безпеки України 2017 року, що вперше системно окреслила національні інтереси в цій сфері [45].

Запровадження правового режиму воєнного стану суттєво зміщує баланс. Закон України «Про правовий режим воєнного стану» допускає тимчасові обмеження конституційних прав, зокрема щодо поширення інформації [41]. У цих умовах звичне індивідуальне балансування за трискладовим тестом доповнюється – а в окремих сегментах і заміщується – категоричними превентивними заборонами.

Найвиразнішим прикладом є стаття 114-2 Кримінального кодексу України [9], запроваджена у 2022 році [18], що встановлює відповідальність за несанкціоноване поширення низки відомостей військового значення, якщо їх не було оприлюднено в офіційний спосіб. Юридична конструкція цієї норми є показовою для всієї проблематики: правомірність поширення прив'язується до критерію попереднього офіційного оприлюднення. Тим самим режим тиші фактично набуває кримінально-правового закріплення для найбільш чутливих категорій інформації, а презумпція відкритості для них тимчасово інвертується: визначальним стає не питання про допустимість обмеження, а питання про наявність офіційного дозволу на розкриття.

Найбільш операційно значущим для повсякденної взаємодії військ із журналістами є тактично-відомчий рівень регулювання, на якому абстрактний баланс відкритості й безпеки перетворюється на конкретні правила роботи медіа. Ці правила закріплюються насамперед наказами Міністерства оборони України та Головнокомандувача Збройних Сил України, затвердженими в різні періоди – від Інструкції про порядок допуску журналістів на об'єкти Міністерства оборони України та Збройних Сил України 2012 року [25] до нормативних документів періоду воєнного стану; їхню еволюцію докладно розглянуто нижче в межах періодизації.

Еволюція нормативно-правового забезпечення періоду (2014–2026)

Нормативно-правове забезпечення інформаційної безпеки не було сталим: воно змінювалося разом із правовим режимом збройного протистояння Росії та України. Три послідовні періоди – антитерористична операція, операція Об'єднаних сил і повномасштабне вторгнення з режимом воєнного стану – відрізняються не лише правовою підставою ведення бойових дій та органом, що ними керує, а й характерною конфігурацією співвідношення відкритості та режиму тиші. Простеження цієї еволюції дає змогу побачити, як безпекова логіка поступово посилювалася, а простір відкритості звужувався, що безпосередньо визначало й умови комунікаційної взаємодії військ із медіа на тактичному рівні.

Період антитерористичної операції (2014–2018)

Правовою основою протидії збройній агресії на цьому етапі стала антитерористична модель. Бойові дії велися у форматі антитерористичної операції, розпочатої навесні 2014 року на підставі рішення Ради національної безпеки і оборони України та відповідно до Закону України «Про боротьбу з тероризмом» [15]; координацію операції здійснював Антитерористичний центр при Службі безпеки України. Юридичним тригером цього етапу став Указ Президента України від 14 квітня 2014 року № 405/2014 [42], який формально запустив оборонні механізми, проте залишив інформаційну сферу у хиткому стані. Правовий режим воєнного стану в цей період не запроваджувався, попри те що профільний Закон України «Про правовий режим воєнного стану» було ухвалено у 2015 році [41] – він залишався «сплячим» інструментом.

Оскільки надзвичайні режими не діяли, інформаційна сфера регулювалася переважно галузевим законодавством мирного часу – законами «Про інформацію» [34] та «Про доступ до публічної інформації» [20] з їхньою презумпцією відкритості й трискладовим тестом. Хоча Закон «Про інформацію» та Закон «Про державну таємницю» формально містили базові обмеження щодо поширення відомостей, які можуть зашкодити нацбезпеці, а Звід відомостей, що становлять державну таємницю, чітко окреслював параметри секретності щодо дислокації та озброєння військ, ці

інструменти виявилися неадаптованими до умов «гібридної» війни в цифрову епоху. Режим тиші існував радше як ситуативна практика командування операції, ніж як юридично оформлений інститут: обмеження щодо висвітлення бойових дій запроваджувалися тимчасово, без окремої нормативної підстави та без кримінально-правового підкріплення. На стратегічному рівні необхідність жорсткішого контролю була усвідомлена лише після перших катастрофічних наслідків «стримів» з фронту. Зокрема, Указ Президента від 24 вересня 2014 року № 744/2014 [44] (реагуючи на трагедію в Іловайську) вперше прямо доручив Кабміну та силовим відомствам посилити контроль за витоком інформації та врегулювати акредитацію журналістів. Водночас саме в цей період закладаються перші спеціальні інструменти захисту національного інформаційного простору – зокрема обмеження ретрансляції ворожого пропагандистського контенту згідно із Законом України «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України» [17], а також інституційне оформлення державної інформаційної політики (створення Міністерства інформаційної політики наприкінці 2014 року).

У площині медіавзаємодії комунікація з журналістами будувалася ситуативно: акредитація та допуск представників медіа в зону операції здійснювалися Антитерористичним центром при Службі безпеки України відповідно до спеціального порядку акредитації представників медіа [11], який запровадив перші паперові перепустки, а офіційне інформування забезпечували прес-центр операції та новостворені підрозділи зі зв'язків із громадськістю, ще без єдиного унормованого порядку. Дискреційний характер цієї моделі був закладений уже в статті 17 Закону України «Про боротьбу з тероризмом» [15], за якою обсяг, форму і час інформування громадськості визначає керівник операції, а єдиним чинним відомчим актом загального характеру тривалий час залишалася Інструкція про порядок допуску журналістів, працівників засобів масової інформації на об'єкти Міністерства оборони України та Збройних Сил України, затверджена наказом Міноборони від 14 червня 2012 року № 399 [25], – документ, розроблений для умов мирного часу й не розрахований на район активних бойових дій.

Першим профільним відомчим актом став наказ Міністерства оборони України від 17.04.2015 № 174 «Про організацію висвітлення діяльності Збройних Сил України» [38]. Лише наприкінці 2016 року з'являється фундаментальний документ цього етапу – Правила роботи представників засобів масової інформації в районі проведення антитерористичної операції [14], внесені наказом першого заступника керівника Антитерористичного центру при Службі безпеки України (керівника АТО) від 27.10.2016 № 555 як додаток 4 до наказу від 19.01.2016 № 45 про упорядкування допуску представників медіа на військові об'єкти; оновлений порядок запрацював із 1 січня 2017 року. Саме цей документ юридично закріпив поняття OPSEC (безпеки операцій) на рівні роботи медіа: увів дворівневу систему акредитації (знамениті «сині» картки для загального допуску та «рожеві» – для передової), встановив правило обов'язкового супроводу пресофіцерами та чітко заборонив фіксацію позицій, техніки й обличь без дозволу. Ще у жовтні 2016 року наказом Генерального штабу ЗСУ від 07.10.2016 № 374 було затверджено Інструкцію з реалізації стратегічних комунікацій у Збройних Силах України [22] – перший відомчий акт, що операціоналізував стратегічні комунікації на рівні війська. Наприкінці періоду АТО цю систему остаточно закріпив наказ Генерального штабу ЗСУ від 11.04.2017 № 127 [29], яким затверджено Положення про органи зв'язків з громадськістю (прес-служби) Збройних Сил України і який перетворив ситуативну роботу пресцентрів на сталу систему зв'язків з громадськістю. Ціну нормативної невизначеності перших років унаочнили події під Іловайськом (серпень 2014 року) та в районі Дебальцевого (січень–лютий 2015 року): оприлюднення в реальному часі відомостей про переміщення військ створювало пряму загрозу життю військовослужбовців, тоді як офіційне применшення масштабів втрат підривало суспільну довіру до державної комунікації та стимулювало розвиток альтернативних, непідконтрольних джерел інформації. Спробою врегулювати цей хаос на рівні тактичного компромісу між армією та медіа стали спільні «Пам'ятки для представників ЗМІ», які, попри свій рекомендаційний характер, підписувалися журналістами як обов'язковий регламент роботи. Доктринальним підсумком періоду стала Доктрина інформаційної безпеки України 2017 року [45], яка вперше системно окреслила національні інтереси, загрози та засади державної політики в інформаційній сфері в умовах гібридної агресії. Того ж року наказом Міністерства оборони України від 22.11.2017 № 612 схвалено Концепцію стратегічних комунікацій Міністерства оборони України та Збройних Сил України [27] – першу концептуальну рамку стратегічних комунікацій оборонного відомства.

Період операції Об'єднаних сил (2018–2022)

Другий період позначений переходом від антитерористичної до оборонної моделі. Із набуттям чинності Законом України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» [40] формат антитерористичної операції було замінено операцією Об'єднаних сил, розпочатою 30 квітня 2018 року. Цей закон докорінно змінив правову логіку оборонного дискурсу: він чітко підпорядкував усі силові структури Командувачу об'єднаних сил та надав військовому керівництву легітимне право встановлювати особливі режими доступу в зону бойових дій. Керівництво силами перейшло від Служби безпеки України до Збройних Сил України – до Об'єднаного оперативного штабу, а протидія агресії дістала кваліфікацію заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації. Ця зміна мала й інформаційно-правовий вимір: комунікація щодо бойових дій дедалі більше інтегрувалася у військову вертикаль.

На системному рівні визначальним став Закон України «Про національну безпеку України» [36], який закріпив інформаційну безпеку як окрему сферу національної безпеки, нормативно визначив принципи стратегічних комунікацій (StratCom) як невіддільного елемента оборони держави та впорядкував сектор безпеки й оборони. Стратегічно-доктринальний рівень оновлюється ухваленням Стратегії інформаційної безпеки [43] з акцентом на стратегічних комунікаціях, інформаційному суверенітеті та протидії дезінформації; інституційно цей курс супроводжується розбудовою спроможностей стратегічних комунікацій, зокрема профільних структур зв'язків із громадськістю у Збройних Силах та Центру стратегічних комунікацій. Інституційне оформлення цієї вертикалі завершили накази Головнокомандувача Збройних Сил України 2020 року, якими затверджено положення про Управління стратегічних комунікацій Апарату Головнокомандувача [32] та про Управління зв'язків з громадськістю Збройних Сил України [31], а в Міністерстві оборони України – Положення про Департамент стратегічних комунікацій (наказ від 09.04.2020 № 114) [28]. Доктринальним підсумком цього курсу стала Доктрина публічного спілкування (ВКП 18-00(01).01), затверджена Головнокомандувачем Збройних Сил України у вересні 2020 року [5], – базовий документ про принципи публічної комунікації війська, розроблений з урахуванням підходів держав – членів НАТО. Важливим кроком у розвитку комунікаційних спроможностей за стандартами НАТО став наказ Генерального штабу ЗСУ від 22.10.2018 № 345 [21], яким затверджено Інструкцію з організації діяльності високомобільних груп внутрішніх комунікацій у Збройних Силах України, що розширило інструментарій військових медіа і пресофіцерів. У вимірі медіавзаємодії функцію офіційного інформування перебирає прес-центр операції Об'єднаних сил, а взаємодія з журналістами поступово формалізується: усталюються процедури акредитації, супроводу та роботи медіа в районі операції, що відображає перехід комунікації військ із медіа від ситуативної моделі до інституційно керованої. Інституційним рубежем стало те, що з 25 квітня 2018 року акредитацію представників медіа почав здійснювати прес-центр Об'єднаних сил, а Служба безпеки України припинила виконання цих функцій.

Центральним документом оперативно-тактичного рівня став Наказ Командувача об'єднаних сил від 23.04.2018 № 20 [12], який затвердив Порядок допуску представників ЗМІ на військові об'єкти в районі проведення ООС. Цим актом було скасовано старі перепустки АТО та сформовано дворівневу систему акредитації: прескарта другого ступеня (синього кольору) надавала право виконувати редакційні завдання в районі операції без доступу до лінії бойового зіткнення, тоді як прескарта першого ступеня (зеленого кольору – *у деяких джерелах згадується як рожева/червона на етапі переходу*), що видавалася після проходження спеціалізованого курсу при Міністерстві оборони України, дозволяла роботу безпосередньо на лінії зіткнення. Обов'язковим елементом моделі став регламентований супровід журналістів офіцерами прес-служб (служб зв'язків з громадськістю).

Паралельно, з метою забезпечення «режиму тиші» та OPSEC, діяв оновлений під формат ООС перелік відомостей, заборонених до розголошення. Журналісти під розписку зобов'язувалися не фіксувати точні географічні координати, номери частин, прізвища командирів тактичної ланки без погодження, а також системи інженерних загороджень та новітні зразки озброєння (як-от перші застосування комплексів Javelin чи БПЛА Bayraktar).

Водночас медіаспільнота піддавала цю модель системній критиці за бюрократизованість і непрозорість: у 2019 році профільні організації публічно заявляли про «ручне керування» акредитацією та вибіркові відмови журналістам, що окреслило головну ваду періоду – збереження широкої

дискреції командування за формально впорядкованої процедури, без юридично визначених підстав для відмови в акредитації та механізму її оскарження. Саме в цей період уперше практично апробовано і сам режим воєнного стану – під час його короткочасного запровадження в низці областей наприкінці 2018 року, що засвідчило дієвість механізму, передбаченого Законом України «Про правовий режим воєнного стану» [41].

Період повномасштабного вторгнення і воєнного стану (2022–2026)

Повномасштабне вторгнення Російської Федерації 24 лютого 2022 року докорінно змінило правову рамку. Якщо у попередні періоди АТО та ООС обмеження свободи слова і діяльності медіа балансували в межах цивільного законодавства мирного часу, то на новому етапі пріоритет операційної безпеки (OPSEC) отримав абсолютне й легітимне домінування. Цьому сприяла нормативна база, напрацьована на попередньому етапі. Інституційна пам'ять та процедури, вибудовані через Наказ Командувача ООС № 20 (супровід, акредитація), стали правовим шаблоном, який дозволив військовому керівництву в перші ж дні великої війни оперативно розгорнути систему регулювання медіа, продемонструвавши переваги повної мілітаризації комунікацій та єдиної жорсткої вертикалі (від Головнокомандувача до пресофіцера тактичної ланки).

Того ж дня, 24 лютого 2022 року, на всій території держави було запроваджено правовий режим воєнного стану – Указом Президента України «Про введення воєнного стану в Україні» № 64/2022 [16], затвердженим Законом України [33] та згодом неодноразово продовжуваним. Уперше в повному обсязі активовано механізм Закону України «Про правовий режим воєнного стану» [41], який допускає тимчасові обмеження конституційних прав, зокрема щодо поширення інформації.

Ключовою новацією стало кримінально-правове закріплення режиму тиші для найбільш чутливих відомостей. Законом України від 24 березня 2022 року [18] Кримінальний кодекс України доповнено статтею 114-2 [9], яка встановила відповідальність за несанкціоноване поширення інформації про переміщення, рух або розміщення Збройних Сил України, якщо таку інформацію не було оприлюднено в офіційний спосіб. Правомірність поширення відомостей військового значення відтоді прив'язується до критерію попереднього офіційного оприлюднення, унаслідок чого презумпція відкритості для цих категорій тимчасово інвертується. Паралельно оновлюється й медійне регулювання: Закон України «Про медіа» [35] кодифікував діяльність суб'єктів у сфері медіа, посилив захист національного інформаційного простору та впорядкував правила поширення контенту в умовах воєнного стану.

На рівні практики режим тиші дістав розгорнуте втілення в системі офіційної комунікації та безпосередньо переформатував взаємодію військ із медіа. Порядок роботи представників медіа в районах ведення бойових дій було унормовано насамперед **наказом Головнокомандувача Збройних Сил України від 3 березня 2022 року № 73** «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» [37] та **наказом Міністерства оборони України від 8 лютого 2022 року № 36** «Про затвердження Інструкції про порядок допуску журналістів, працівників засобів масової інформації на об'єкти системи Міністерства оборони України» [26], – що запровадили обов'язкову акредитацію, поділ території на зони доступу та супровід журналістів офіцерами зі зв'язків із громадськістю. Наказ № 36 затвердив порядок допуску журналістів і працівників медіа на об'єкти системи Міністерства оборони та прямо передбачає дотримання ними режиму доступу до інформації з обмеженим доступом. Наказ № 73 став базовим документом періоду повномасштабного вторгнення і має декілька редакцій зі змінами, внесеними наказами Головнокомандувача ЗСУ № 196 від 12.07.2022, № 266 від 03.10.2022, № 49 від 27.02.2023, № 51 від 03.02.2024 та № 31 від 17.01.2025. Первинна редакція наказу № 73 визначила алгоритм дій командувачів і командирів під час роботи з цивільними медіа, порядок акредитації журналістів національних та іноземних медіа і правила роботи представника медіа в районі ведення бойових дій; окремим додатком закріплено перелік відомостей, розголошення яких заборонене. Наказ № 73 також скасував старі перепустки операції Об'єднаних сил, запровадив єдину акредитацію ЗСУ та чітко визначив перелік відомостей, які категорично заборонено розголошувати (чисельність і назви частин, геолокація позицій, наслідки ударів до закінчення встановленого терміну мовчання).

Суттєві зміни до наказу № 73 внесено наказом Головнокомандувача ЗСУ від 27.02.2023 № 49, яким структуровано зону бойових дій на три зони доступу: «зелену» (вільна робота медіа), «жовту» (робота лише у супроводі пресофіцера) та «червону» (повна заборона доступу). Тоді ж

запроваджено прескарту нового зразка строком до шести місяців і можливість призупинення акредитації на час з'ясування обставин порушення. Надання командувачам оперативно-стратегічних угруповань військ (ОСУВ) права щотижня змінювати статус населених пунктів на тактичному рівні фактично закрило передову для незалежної журналістики, перевівши більшість гарячих точок у «червону зону». Це зумовило глибоку кризу у відносинах ЗСУ з вітчизняними та іноземними медіа.

Показово, що ця нормативна база формувалася в діалозі з медіаспільнотою. Каталізатором перегляду стало резонансне позбавлення акредитації низки українських та іноземних журналістів за роботу в щойно деокупованому Херсоні в листопаді 2022 року, після якого було створено робочі групи за участю журналістів, профільних громадських організацій, представників Збройних Сил, Генерального штабу та Офісу Президента.

Наступні зміни були закріплені в наказі Головнокомандувача ЗСУ від 3 лютого 2024 року № 51 і мали переважно ліберальний характер: строк акредитації подовжено до дванадцяти місяців, чітко описано межі та правила кожної із зон, спрощено погодження інтерв'ю (дозвіл надає прямий командир, а не вище командування), передбачено акредитацію суб'єктів у сфері онлайн-медіа, зареєстрованих відповідно до Закону України «Про медіа» [35], і водночас розширено та конкретизовано перелік відомостей, заборонених до розголошення. Аналітичні структури (наприклад Інститут масової інформації), які моніторять свободу слова, фіксували як здобутки оновленого наказу № 73 (лібералізацію зон доступу, посилення гарантій безпеки журналістів, узгодження із Законом «Про медіа» [35]), так і невирішені суперечності – насамперед відсутність розмежування дозволу на зйомку та дозволу на публікацію, ризик надмірного розширення червоних зон і вибірковість доступу до них.

Останні за часом зміни, закріплені наказом Головнокомандувача ЗСУ від 17 січня 2025 року № 31, завершили трансформацію системи зонування шляхом суттєвої децентралізації доступу медіа. Зокрема, було скасовано вимогу щодо обов'язкового супроводу пресофіцера під час роботи журналістів у цивільних локаціях та громадських місцях всередині «жовтої» зони, дозволивши акредитованим медійникам працювати там самостійно; регламентовано механізм точкового допуску до «червоної» зони у виняткових випадках за розпорядженням командування угруповань військ і в супроводі офіційних осіб; уточнено положення щодо верифікації медіа та актуалізовано додаток із переліком відомостей, несанкціоноване поширення яких шкодить операційній безпеці (зокрема щодо фіксації засобів РЕБ, ППО та точних координат дислокацій).

У термінах співвідношення відкритості й режиму тиші наказ № 73 у його чинній редакції (з урахуванням усіх наведених змін) є найточнішим нормативним втіленням балансу: система зон операціоналізує контрольовану відкритість (керований доступ замість суцільної заборони чи безконтрольного допуску), а перелік заборонених відомостей є юридичною формалізацією критично важливої інформації в логіці операційної безпеки. Ця еволюція унаочнює, що українська модель є моделлю контрольованої відкритості, яка виробляється в постійному узгодженні інтересів, а не статичним набором заборон.

Протягом 2024–2026 років Наказ № 73 продовжував еволюціонувати в бік врегулювання нових технологічних ризиків. До нього було внесено суворі обмеження щодо використання супутникових систем (Starlink) журналістами безпосередньо на позиціях, правила роботи цивільних дронів у зоні відповідальності бригад, а також запроваджено цифровізацію та верифікацію процесу акредитації. Одночасно держава посилила внутрішній OPSEC через директиви Генерального штабу ЗСУ щодо суворої регламентації використання смартфонів, зйомок на позиціях та ведення особистих соцмереж (TikTok, Telegram) самими військовослужбовцями (нормативним попередником тут була Інструкція зі зберігання і користування особовим складом засобами стільникового зв'язку, затверджена наказом Головнокомандувача ЗСУ від 01.07.2020 № 74 [23]), контроль за чим частково ліг на служби зв'язків з громадськістю (СЗГ) бригад.

Офіційне інформування централізувалося – від скоординованого оприлюднення відомостей уповноваженими органами до формування спільного інформаційного марафону як загальнонаціонального майданчика новин. Характер періоду – домінування безпекової логіки: індивідуальне балансування за трискладовим тестом доповнюється, а подекуди й заміщується категоричними превентивними заборонами, а режим тиші фактично інституціоналізується як робоче правило журналістської практики, хоч і залишається без автономного легального визначення.

Водночас інституційне оновлення комунікаційної вертикалі свідчить про поступове врівноваження цього зміщення: наказом Головнокомандувача

Збройних Сил України від 10 червня 2025 року № 284 затверджено Положення про підрозділи комунікацій Збройних Сил України [30]. Цей наказ прийшов на заміну одразу двом актам: наказ Головнокомандувача ЗСУ від 18 березня 2023 року № 70 «Про затвердження Порядку здійснення стратегічних комунікацій Збройних Сил України» визнано таким, що втратив чинність, а наказ Генерального штабу від 11 квітня 2017 року № 127 «Про затвердження Положення про органи зв'язків з громадськістю (прес-служби) Збройних Сил України» [29] – таким, що не застосовується. Доктринальну лінію продовжила Доктрина «Військові зв'язки з громадськістю» (ОП 10-0(208), AJP-10.3), затверджена начальником Генерального штабу 15 січня 2026 року [3], – друге видання, яке замінило Доктрину публічного спілкування 2020 року [5] і розроблене на основі однойменної союзницької доктрини військових зв'язків з громадськістю AJP-10.3. У координатах співвідношення відкритості й тиші ця доктрина закріплює на відомчому рівні саме презумпцію відкритості: відповідно до натівського принципу максимального розкриття за мінімальної затримки проактивне, своєчасне і правдиве інформування визначено обов'язком підрозділів комунікацій, а утримання від оприлюднення допускається як точковий виняток щодо відомостей, захищених вимогами операційної безпеки. Наказ № 284 відповідає на це питання інституційно: затверджене ним Положення покладає на підрозділи комунікацій обидві складові балансу. З одного боку – проактивну відкритість: інформування громадськості та медіа, «заходи проактивної комунікації» із забезпеченням «статусу першоджерела інформації в умовах кризових ситуацій і реагування на випередження», участь у забезпеченні доступу до публічної інформації; з іншого – заходи інформаційної безпеки щодо «недопущення висвітлення відомостей, які можуть призвести до обізнаності противника», зокрема погодження аудіовізуальних матеріалів і контроль за змістом інформації, яка надається медіа [31]. Конкретні ж межі закритого (зони доступу, перелік заборонених до розголошення відомостей) визначає наказ № 73 [37]. Отже, нормативне оновлення 2025–2026 років не повертає модель до замовчування, а нормативно оформлює контрольовану відкритість: розкривати за замовчуванням, мовчати – лише тоді й тією мірою, якою цього вимагає безпека операцій і людей.

Зіставлення трьох періодів виявляє послідовну траєкторію: від фрагментарного регулювання з переважанням відкритості (антитерористична операція) через мілітаризацію управління й посилення безпекових засад (операція Об'єднаних сил) до кодифікованого обмеження з домінуванням безпекової логіки (воєнний стан). Баланс відкритості й режиму тиші поступово зміщувався в бік тиші, однак у межах третього періоду ця динаміка виявилася нелінійною, коливальною: пікове звуження відкритості 2022 – початку 2023 року змінилося частковою лібералізацією 2024 року, досягнутою через інституціоналізований діалог командування з медіаспільнотою, у якому кризові кейси правозастосування виконували функцію тригерів нормативних змін. Саме тому потреба в законному визначенні цього режиму стала особливо нагальною. Ця періодизація безпосередньо кореспондує із завданнями дисертаційного дослідження, присвяченого еволюції комунікаційної взаємодії Збройних Сил України з медіа на тактичному рівні у 2014–2026 роках.

Європейські та євроатлантичні орієнтири

Національне регулювання має узгоджуватися з міжнародними стандартами. Стаття 10 Конвенції про захист прав людини і основоположних свобод гарантує свободу вираження поглядів і водночас допускає її обмеження, якщо воно встановлене законом, переслідує легітимну мету (зокрема національну безпеку) і є необхідним у демократичному суспільстві [7]. Останній критерій передбачає пропорційність: обмеження не може бути ширшим, ніж це потрібно для досягнення мети. Цей підхід концептуально збігається з національним трискладовим тестом і слугує запобіжником проти надмірних обмежень.

У євроатлантичному вимірі орієнтиром є доктринальні стандарти стратегічних комунікацій НАТО – Об'єднана доктрина зі стратегічних комунікацій AJP-10 [48] і Військова політика НАТО зі стратегічних комунікацій MC 0628 [50], а також уніфіковане тлумачення базових термінів, зокрема операційної безпеки, у Глосарії термінів і визначень НАТО AAP-06 [47]. Ці документи інтегрують захист інформації в ширшу систему узгодженого впливу й публічної діяльності та водночас послідовно дотримуються принципу максимального розкриття за мінімальної затримки, розглядаючи своєчасну й правдиву комунікацію як стратегічний інструмент, а не лише інформаційний супровід. Методологічним доповненням є американська доктрина операційної безпеки Joint Publication 3-13.3, що описує OPSEC як циклічний аналітичний процес оцінювання власної діяльності з позиції противника [49]. Україна сприйняла цю рамку концептуально, зокрема через Доктрину зі стратегічних комунікацій [4] та Доктрину публічного

спілкування [5] Збройних Сил України, проте її інституційне втілення залишається процесом, що триває, і стикається з труднощами – насамперед із потребою узгодити категоричні заборони воєнного часу з вимогою пропорційності та з браком сталих процедур контрольованого розкриття інформації.

Порівняння національних моделей взаємодії армії з медіа дає змогу точніше позиціонувати українське рішення. Американський підхід еволюціонував від жорстких медіа-пулів війни в Перській затоці до програми «вбудованої» журналістики (embedded journalism) в Іраку, за якої доступ до підрозділів надавався в обмін на дотримання заздалегідь визначених правил (Ground Rules) [51]. Ізраїльська модель спирається на превентивну військову цензуру, а британська посідає проміжне положення, регулюючи взаємодію з пресою через узгоджувальний документ «Зелена книга» [52]. На тлі цього спектра українська модель постає як контрольована відкритість: вона свідомо уникає інституту суцільної превентивної цензури, але й не зводиться до необмеженого доступу, поєднуючи узгоджувальні домовленості та «вбудований» доступ із обмеженим переліком заборонених до розголошення відомостей і саморегуляцією медіаспільноти.

Проведений аналіз дає змогу виокремити кілька системних проблем. По-перше, режим тиші застосовується як усталений інструмент, проте не має легального визначення й самостійного статусу, що породжує невизначеність щодо його підстав, суб'єктів, обсягу та строків. По-друге, зберігається колізія між галузевою презумпцією відкритості й безпековою презумпцією обмеження, яка особливо загострюється в умовах дії категоричних заборон. По-третє, бракує єдиних процедур, які забезпечували б своєчасне зняття обмежень і повернення до відкритості після зникнення безпекових підстав.

З огляду на це доцільними є такі напрями вдосконалення. Перший – легальне закріплення режиму тиші як строкового, обмеженого за обсягом і підконтрольного інструмента з чітко визначеними підставами, суб'єктами рішень і механізмом припинення, зокрема через прив'язку розкриття до офіційного підтвердження. Другий – послідовне підпорядкування будь-яких обмежень критерію пропорційності, що дає змогу узгодити галузеву й безпекову логіки та уникнути як надмірних, так і недостатніх обмежень. Третій – розбудова інституту стратегічних комунікацій, який запобігає утворенню інформаційного вакууму й тим самим знижує потребу в обмеженнях. Четвертий – гармонізація національного регулювання з європейськими стандартами свободи вираження поглядів і доктринами стратегічних комунікацій НАТО. Реалізація цих напрямів дала б змогу перетворити співвідношення відкритості й режиму тиші з джерела правової невизначеності на керований, передбачуваний баланс.

Висновки. Дослідження підтверджує, що нормативно-правове забезпечення інформаційної безпеки є багаторівневою системою, у якій відкритість і режим тиші виступають не випадковими, а структурно пов'язаними елементами єдиного механізму балансування. Інформаційна безпека постає як дворівневий об'єкт правового регулювання, що поєднує захист інформаційних прав особи із захистом суспільства й держави від інформаційних загроз, а тому потребує не простого обмеження, а зваженого узгодження різноспрямованих інтересів.

Установлено, що ключову напругу системи становить співіснування галузевої презумпції відкритості та безпекової презумпції обмеження. Аналіз нормативної бази трьох періодів – антитерористичної операції (2014–2018), операції Об'єднаних сил (2018–2022) та повномасштабного вторгнення і воєнного стану (2022–2026) – засвідчує послідовне зміщення балансу від переважання відкритості до безпекового обмеження: у звичайних умовах узгодження здійснювалося через індивідуальне балансування за трискладовим тестом і критерієм пропорційності, тоді як в умовах воєнного стану баланс зміщується в бік категоричних превентивних заборон, найвиразнішим утіленням яких є стаття 114-2 Кримінального кодексу України. Сам режим тиші при цьому залишається юридично невизначеним інститутом, що знижує правову передбачуваність.

Перспективними напрямами подальших досліджень є розроблення правових критеріїв правомірності режиму тиші, механізмів своєчасного зняття інформаційних обмежень та емпіричний аналіз практики застосування відповідних норм, що безпосередньо кореспондує із завданнями дисертаційного дослідження, присвяченого дихотомії інформаційної відкритості й безпеки та еволюції комунікаційної взаємодії Збройних Сил України з медіа на тактичному рівні.

Інформація про використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту використовувалися виключно для мовного редагування, перевірки граматики, перекладу або інших допоміжних завдань, без використання згенерованих ними об'єктів як результатів академічної діяльності.

Список літератури:

1. Баровська А. В. Стратегічні комунікації: досвід НАТО. *Стратегічні пріоритети.* 2015. № 1 (34). С. 147–152.

2. Гребньов Г. Журналістика в умовах воєнного стану: законодавчі норми та професійні стандарти. *Український інформаційний простір*. 2026. № 1 (17). С. 18–35. DOI: https://doi.org/10.31866/2616-7948.1(17).2026.359164.

3. Доктрина «Військові зв'язки з громадськістю» : ОП 10-0(208), AJP-10.3 / Генеральний штаб Збройних Сил України. Київ, 2026. 48 арк.

4. Доктрина зі стратегічних комунікацій : ВКП 10-00(49).01 / Збройні Сили України. Київ, 2020. 36 с.

5. Доктрина публічного спілкування : ВКП 18-00(01).01 / Збройні Сили України. Київ, 2020. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/doktrina-publichnogo-spilkuvannya-serpen-2020 (дата звернення: 01.07.2026).

6. Іжутова І. В. Стратегічні комунікації України в умовах російсько-української війни. *Наука і оборона*. 2023. № 2. С. 46–51. DOI: https://doi.org/10.33099/2618-1614-2023-22-2-46-51.

7. Конвенція про захист прав людини і основоположних свобод : міжнар. договір від 4 листоп. 1950 р. (ст. 10). URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 01.07.2026).

8. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 01.07.2026).

9. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 02.07.2026).

10. Попова Т. В., Ліпкан В. А. Стратегічні комунікації : словник / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2016. 416 с.

11. Порядок акредитації представників засобів масової інформації в районі АТО. Міністерство закордонних справ України : офіційний сайт. URL: https://edinburgh.mfa.gov.ua/news/34555-poryadok-akreditaciji-predstavnikiv-zasobiv-masovoji-informaciji-v-rajoni-ato (дата звернення: 02.07.2026).

12. Порядок допуску представників засобів масової інформації на військові об'єкти у районі проведення операції об'єднаних сил : наказ Командувача об'єднаних сил від 23 квіт. 2018 р. № 20.

13. Почепцов Г. Сучасні інформаційні війни. Київ : Вид. дім «Києво-Могилянська академія», 2015. 497 с.

14. Правила роботи представників засобів масової інформації в районі проведення антитерористичної операції : дод. 4 до наказу Антитерористичного центру при Службі безпеки України (керівника Антитерористичної операції на території Донецької та Луганської областей) від 19 січ. 2016 р. № 45 «Про упорядкування порядку допуску представників засобів масової інформації на військові об'єкти у районі проведення Антитерористичної операції на території Донецької та Луганської областей» ; дод. внесено наказом першого заступника керівника Антитерористичного центру при Службі безпеки України від 27 жовт. 2016 р. № 555.

15. Про боротьбу з тероризмом : Закон України від 20 берез. 2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 01.07.2026).

16. Про введення воєнного стану в Україні : Указ Президента України від 24 лют. 2022 р. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022 (дата звернення: 01.07.2026).

17. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України : Закон України від 5 лют. 2015 р. № 159-VIII. URL: https://zakon.rada.gov.ua/laws/show/159-19 (дата звернення: 02.07.2026).

18. Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо забезпечення протидії несанкціонованому поширенню інформації про переміщення, рух або розміщення Збройних Сил України : Закон України від 24 берез. 2022 р. № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20 (дата звернення: 01.07.2026).

19. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 01.07.2026).

20. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 01.07.2026).

21. Про затвердження Інструкції з організації діяльності високомобільних груп внутрішніх комунікацій у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 22 жовт. 2018 р. № 345. URL: https://dovidnykmpz.info/zagalni/nakaz-heneral-noho-shtabu-zs-ukrainy-v-2/ (дата звернення: 01.07.2026).

22. Про затвердження Інструкції з реалізації стратегічних комунікацій у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 7 жовт. 2016 р. № 374.

23. Про затвердження Інструкції зі зберігання і користування особовим складом Збройних Сил України засобами стільникового зв'язку та іншими електронними засобами : наказ Головнокомандувача Збройних Сил України від 1 лип. 2020 р. № 74.

24. Про затвердження Інструкції із забезпечення доступу до публічної інформації в Міністерстві оборони України та Збройних Силах України : наказ Міністерства оборони України від 13 черв. 2017 р. № 319, зареєстр. в М-ві юстиції України 6 лип. 2017 р. за № 827/30695. URL: https://zakon.rada.gov.ua/laws/show/z0827-17 (дата звернення: 01.07.2026).

25. Про затвердження Інструкції про порядок допуску журналістів, працівників засобів масової інформації на об'єкти Міністерства оборони України та Збройних Сил України : наказ Міністерства оборони України від 14 черв. 2012 р. № 399, зареєстр. в М-ві юстиції України 9 лип. 2012 р. за № 1149/21461 (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/z1149-12 (дата звернення: 09.07.2026).

26. Про затвердження Інструкції про порядок допуску журналістів, працівників засобів масової інформації на об'єкти системи Міністерства оборони України : наказ Міністерства оборони України від 8 лют. 2022 р. № 36. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-ministerstva-oboroni-ukraini-n-36-vid-08-02-2022-pro-zatverdzhennia-instruktsii-pro-poriadok-dopusku-zhurnalistiv-pratsivnikiv-zasobiv-masovoi-informatsii-na-ob-iekti-sistemi-ministerstva (дата звернення: 08.07.2026).

27. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України : наказ Міністерства оборони України від 22 листоп. 2017 р. № 612.

28. Про затвердження Положення про Департамент стратегічних комунікацій Міністерства оборони України : наказ Міністерства оборони України від 9 квіт. 2020 р. № 114.

29. Про затвердження Положення про органи зв'язків з громадськістю (прес-служби) Збройних Сил України : наказ Генерального штабу Збройних Сил України від 11 квіт. 2017 р. № 127.

30. Про затвердження Положення про підрозділи комунікацій Збройних Сил України : наказ Головнокомандувача Збройних Сил України від 10 черв. 2025 р. № 284.

31. Про затвердження Положення про Управління зв'язків з громадськістю Збройних Сил України : наказ Головнокомандувача Збройних Сил України від 3 черв. 2020 р. № 44.

32. Про затвердження Положення про Управління стратегічних комунікацій Апарату Головнокомандувача Збройних Сил України : наказ Головнокомандувача Збройних Сил України від 14 квіт. 2020 р. № 14.

33. Про затвердження Указу Президента України «Про введення воєнного стану в Україні» : Закон України від 24 лют. 2022 р. № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20 (дата звернення: 01.07.2026).

34. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 01.07.2026).

35. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20 (дата звернення: 01.07.2026).

36. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 01.07.2026).

37. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану : наказ Головнокомандувача Збройних Сил України від 3 берез. 2022 р. № 73 (зі змінами згідно з наказами від 12 лип. 2022 р. № 196, від 3 жовт. 2022 р. № 266, від 27 лют. 2023 р. № 49, від 3 лют. 2024 р. № 51 та від 17 січ. 2025 р. № 31). URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-golovnokomanduvacha-zsu-vid-03-03-2022-roku-73-zi-zminami (дата звернення: 09.07.2026).

38. Про організацію висвітлення діяльності Збройних Сил України : наказ Міністерства оборони України від 17 квіт. 2015 р. № 174.

39. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.07.2026).

40. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях : Закон України від 18 січ. 2018 р. № 2268-VIII. URL: https://zakon.rada.gov.ua/laws/show/2268-19 (дата звернення: 01.07.2026).

41. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 01.07.2026).

42. Про рішення Ради національної безпеки і оборони України від 13 квітня 2014 року «Про невідкладні заходи щодо подолання терористичної загрози і збереження територіальної цілісності України» : Указ Президента України від 14 квіт. 2014 р. № 405/2014. URL: https://zakon.rada.gov.ua/laws/show/405/2014 (дата звернення: 01.07.2026).

43. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 01.07.2026).

44. Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності» : Указ Президента України від 24 верес. 2014 р. № 744/2014. URL: https://zakon.rada.gov.ua/laws/show/744/2014 (дата звернення: 01.07.2026).

45. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 09.07.2026).

46. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.

47. AAP-06. NATO Glossary of Terms and Definitions (English and French). Edition 2021. Brussels : NATO Standardization Office, 2021. https://english-military-dictionary.org.ua/search/OPSEC?84947d1f5d45e3f2ac6a2b5561fc0d38=1 (дата звернення: 10.07.2026).

48. AJP-10. Allied Joint Doctrine for Strategic Communications. Edition A, Version 1. NATO Standardization Office, 2023. 184 p. https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата звернення: 09.07.2026).

49. Joint Publication 3-13.3. Operations Security. Washington : Joint Chiefs of Staff, 2016. URL: https://media.defense.gov/2020/Oct/28/2002524944/-1/-1/0/JP%203-13.3-OPSEC.PDF (дата звернення: 09.07.2026).

50. NATO Military Policy on Strategic Communications (MC 0628). Brussels : NATO, 2017.

51. Public Affairs Guidance (PAG) on Embedding Media during Possible Future Operations/Deployments in the U.S. Central Command Area of Responsibility. Washington : U.S. Department of Defense, 2003.

52. The Green Book: MOD Working Arrangements with the Media for Use throughout the Full Spectrum of Conflict. Version 8. London : Ministry of Defence, 2013.

Rozhniativska N.V. REGULATORY AND LEGAL FRAMEWORK FOR INFORMATION SECURITY: THE BALANCE BETWEEN TRANSPARENCY AND CONFIDENTIALITY (2014–2026)

This article analyzes Ukraine's legal framework for information security as the direct regulator of communication between the Armed Forces of Ukraine and the media, which operates at the intersection of information transparency and a media blackout. The legal mechanism for balancing openness and restrictions is characterized as a multilevel system encompassing constitutional, legislative, strategic-doctrinal, special (martial law), and tactical-departmental levels of regulation. It is demonstrated that the legal regime governing access to information about the course of hostilities determines the day-to-day conditions of media operations in the combat zone: the procedure for accrediting journalists, access zones, limits on reporting the movement and deployment of troops, and the formats of official communication by the security and defense sector. The main focus is on the evolution of the regulatory framework and media engagement practices across three periods of armed conflict: the anti-terrorist operation (2014–2018), the Joint Forces Operation (2018–2022), and the full-scale invasion and martial law (2022–2026). It was found that the balance shifted progressively from a predominance of openness toward security-based restrictions, however, within the framework of martial law, this dynamic was not linear: the peak restriction of openness in 2022–2023 was followed by a partial liberalization in 2024–2025, achieved through institutionalized dialogue between the command and the media community. A contradiction has been identified between the presumption of openness of public information and the security rationale for preventive restrictions, as well as legal uncertainty regarding the "silence regime," which is applied as an established tool but lacks a legal definition, thereby reducing legal predictability for all participants in communication interactions. The following areas for improvement are proposed: legally enshrining the "silence regime" as a time-limited, scope-limited, and controllable tool; consistently subjecting any information restrictions to the principle of proportionality; developing the institution of strategic communications to prevent the creation of an information vacuum; harmonizing national regulations with European standards on freedom of expression and NATO's doctrines of strategic communications.

Keywords: *information security, strategic communications, media relations, transparency, operational security (OPSEC), media blackout, journalist accreditation, martial law.*

Дата першого надходження статті до видання: 04.08.2026
Дата прийняття статті до друку після рецензування: 02.09.2026
Дата публікації (оприлюднення) статті: 23.10.2026