

DOI 10.31558/2519-2949.2025.3.15

УДК 355.45:004.056.5(477)

ORCID ID: <https://orcid.org/0000-0002-4471-2400>**Пашковський В. Ф., Київський національний університет імені Тараса Шевченка**

ІДЕНТИФІКАЦІЯ ПОЛІТИКО-ПРАВОВИХ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У статті здійснено комплексне дослідження політико-правових механізмів інформаційної політики держави в умовах гібридної війни. Показано, що інформаційна політика України розвивається в контексті поєднання правових норм, стратегічних документів та інституційних практик, спрямованих на протидію інформаційним загрозам. У роботі: ідентифіковано ключові теоретико-концептуальні засади дослідження інформаційної політики та її зв'язку з категоріями інформаційної безпеки й гібридної війни; проаналізовано нормативно-правову базу України (Конституція, закони, укази Президента, стратегії), а також міжнародні стандарти (DSA, EDAP, Кодекс практик проти дезінформації, документи НАТО StratCom COE та ЄС); визначено інституційно-організаційні механізми, серед яких діяльність РНБО, Міністерства культури та інформаційної політики, Центру протидії дезінформації, а також роль громадянського суспільства та міжнародних партнерів; систематизовано політико-правові інструменти: «жорсткі» (санкції, блокування ресурсів, регулювання медіа) та «м'які» (стратегічні комунікації, інформаційні кампанії, фактчекінг); сформульовано перспективи та рекомендації щодо вдосконалення інформаційної політики: гармонізація законодавства з європейськими стандартами, створення єдиної координаційної структури, розвиток суспільної стійкості та інтеграція в євроатлантичний безпековий простір. З'ясовано, що ефективність інформаційної політики держави у протидії гібридним загрозам можлива лише за умови синергії політико-правових норм, інституційної координації та стратегічних комунікацій. Загалом, політико-правові механізми інформаційної політики в умовах гібридної війни повинні функціонувати як система взаємодії права, інституцій та стратегічних комунікацій, що дозволить державі не лише протистояти загрозам, але й формувати власний позитивний інформаційний простір.

Ключові слова: інформаційна політика, політико-правові механізми, гібридна війна, інформаційна безпека, стратегічні комунікації, дезінформація, нормативно-правове регулювання.

Постановка питання. Сучасні умови гібридної війни, що розгортається навколо України з 2014 року та особливо після повномасштабного вторгнення Російської Федерації у 2022 році, висувають нові вимоги до формування та реалізації інформаційної політики держави. Інформаційна сфера стає не лише простором комунікації, а й ареною стратегічного протистояння, де вирішуються питання національної безпеки, політичної стабільності та міжнародного іміджу держави. Саме тому дослідження політико-правових механізмів інформаційної політики є надзвичайно актуальним для розуміння можливостей протидії інформаційним загрозам і побудови стійкої моделі інформаційної безпеки.

Українські науковці наголошують, що саме інформаційний компонент є найбільш вразливою сферою національної безпеки, адже він тісно пов'язаний із суспільною довірою, демократичними інститутами та міжнародною репутацією держави [1, с. 7–9]. Західні дослідники відзначають, що гібридна війна передбачає комплексне використання військових, політичних, економічних, інформаційних і кібернетичних інструментів з метою досягнення стратегічних переваг без оголошення класичної війни [2, р. 29].

Аналіз останніх досліджень і публікацій. У вітчизняному науковому просторі проблематику політико-правових механізмів інформаційної політики досліджують такі автори, як Л. Компанцева, яка розглядає доктрину інформаційної безпеки України в теоретико-правовому аспекті [1]; А. Антипова, яка аналізує стратегічні комунікації як складову державної інформаційної безпеки [3]; О. Зернецька, котра підкреслює глобальні виклики інформаційного суспільства та вплив світових

комунікаційних процесів на державну політику [4].

Серед зарубіжних досліджень важливими є роботи Ф. Хофмана, що заклав теоретичні основи розуміння гібридної війни [2]; Б. Хоскінса та Б. О'Лафліна, які аналізують феномен «дифузної війни» у медійному просторі [5], а також аналітичні документи НАТО StratCom COE [6; 7], де систематизовано інструменти російських інформаційних кампаній.

Таким чином, проблематика інформаційної політики в умовах гібридної війни має як глибокі теоретичні напрацювання, так і практичне значення для забезпечення національної безпеки.

Метою статті є ідентифікація та концептуалізація політико-правових механізмів інформаційної політики держави в умовах гібридної війни, визначення їх ефективності та обмежень, а також формування рекомендацій для оптимізації системи правового регулювання в Україні з урахуванням міжнародного досвіду. Приводом для написання стала необхідність комплексного теоретичного аналізу, адже більшість існуючих досліджень фрагментарно зосереджені або на безпековому, або на правовому аспекті. Натомість інтегрований підхід дає змогу чітко окреслити механізми, що поєднують правові норми, інституційні практики та стратегічні комунікації в єдину систему протидії інформаційним загрозам.

Методи дослідження. У дослідженні застосовано комплекс методів. Так, системний підхід – дозволив розглядати інформаційну політику як цілісну систему, що поєднує правові норми, інститути та практики у протидії гібридним загрозам; порівняльно-правовий метод – надав можливість зіставити українське законодавство із європейськими та міжнародними нормативними актами (зокрема, Digital Services Act, NATO StratCom COE policy). Це дало підстави окреслити тенденції адаптації українських механізмів до європейських стандартів; контент-аналіз документів стратегічного характеру (доктрини, стратегії, укази) – дозволив виокремити ключові правові механізми регулювання інформаційної сфери; інституційний аналіз – допоміг визначити функції та ефективність державних і міжнародних органів у сфері інформаційної політики. У сукупності ці методи дали змогу не лише описати політико-правові механізми, а й оцінити їхню дієвість у конкретних умовах гібридної війни.

Виклад основного матеріалу. Поняття «інформаційна політика держави» у науковій літературі визначається по-різному, проте спільним є її розуміння як комплексу заходів і рішень, спрямованих на регулювання інформаційних процесів у суспільстві та забезпечення інформаційної безпеки. Так, О. Зернецька наголошує, що «інформаційна політика має подвійний характер: з одного боку, вона відображає прагнення держави інтегруватися у світовий інформаційний простір, а з іншого – потребу захистити національний інформаційний суверенітет» [4, с. 215]. Л. Компанцева визначає її як «систему правових, організаційних та комунікаційних механізмів, що забезпечують реалізацію стратегічних інтересів держави у сфері інформації» [1, с. 6]. На думку західних дослідників, інформаційна політика сучасних демократій має балансувати між свободою слова та захистом суспільства від дезінформації, особливо в умовах гібридних загроз [8, р. 43–45]. Таким чином, інформаційна політика в нашому дослідженні розглядається як поєднання правових норм, стратегічних програм та інституційних практик, спрямованих на забезпечення інформаційної стійкості держави.

Інформаційна безпека традиційно розглядається як ключовий вимір інформаційної політики. Конституція України та Закон «Про національну безпеку» визначають інформаційну безпеку як одну з основних складових національної безпеки [9]. А. Антипова підкреслює, що у контексті гібридної війни інформаційна безпека набуває рис стратегічних комунікацій, адже йдеться не лише про захист інфраструктури, а й про здатність формувати та транслювати власні наративи [3, с. 45]. Західні дослідники вказують, що у XXI ст. безпека визначається не стільки військовими, скільки інформаційними та когнітивними факторами [10, р. 238–240]. Отже, інформаційна безпека – це не тільки правовий та технічний захист, але й комунікаційна спроможність держави.

Щодо терміну «гібридна війна», то він був концептуалізований у працях американського дослідника Ф. Хофмана, який визначав її як поєднання традиційних та нетрадиційних методів боротьби, де особлива роль відводиться інформаційним та психологічним операціям [2, р. 30]. У випадку України гібридна війна означає використання Росією інформаційних кампаній, кібератак, економічного тиску та військових дій для досягнення політичних цілей. Дослідження StratCom COE [6] показують, що російські інформаційні операції базуються на довготривалому створенні паралельної реальності через медіа та соціальні мережі, спрямовані на підірив довіри до демократичних інститутів.

Українські вчені, наприклад, К. Грищенко, підкреслюють, що ключова загроза гібридної війни полягає у дестабілізації політико-правового порядку держави через маніпулятивні інформаційні технології [11, с. 18-20].

Отже, теоретико-концептуальні засади показують, що інформаційна політика, інформаційна безпека та гібридна війна утворюють єдиний аналітичний трикутник. Без чіткого правового та інституційного закріплення інформаційної політики неможливо протистояти інформаційним аспектам гібридної агресії.

Нормативно-правові засади інформаційної політики держави. Конституція України закріплює основи інформаційної політики через гарантії свободи слова, доступу до інформації та права на захист особистих даних. Стаття 34 визначає право кожного на свободу думки й слова, а також на вільне збирання, зберігання та поширення інформації. Водночас стаття 17 підкреслює, що забезпечення інформаційної безпеки є складовою національної безпеки держави [12]. Це створює подвійний нормативний баланс: між гарантіями демократичних свобод і потребою в захисті держави від інформаційних загроз.

Ключовими спеціальними законами є:

- Закон України «Про інформацію» (1992, ред. 2024 р.) — закладає загальні принципи доступу, збирання та поширення інформації, визначає права й обов'язки суб'єктів інформаційних відносин. В останніх редакціях наголошено на необхідності захисту від дезінформації та маніпуляцій (ст. 47) [13];

- Закон України «Про медіа» (2022 р.) — став важливим кроком у гармонізації українського законодавства з європейськими стандартами. Він запроваджує механізми регулювання онлайн-платформ, прозорість власності медіа та відповідальність за поширення забороненого контенту (ст. 118–122) [14];

- Закон України «Про національну безпеку» (2018 р.) — визначає інформаційну безпеку як один із пріоритетних напрямів національної безпеки, що охоплює протидію пропаганді, дезінформації та кіберзагрозам (ст. 3, п. 7) [15].

Як слушно зауважує Л. Компанцева, правове регулювання інформаційної політики в Україні має системний характер, однак залишається фрагментарним у частині конкретних механізмів протидії інформаційним операціям [1, с. 8–9]. Західні дослідники теж зазначають, що для сучасних демократій проблемою є не стільки наявність правових норм, скільки їхня дієвість у цифровому середовищі, де традиційні інструменти правового контролю часто втрачають ефективність [8, р. 46].

Окрім базових законів, вагому роль у формуванні політико-правових механізмів інформаційної політики відіграють акти Президента України та стратегічні документи, які задають орієнтири державної діяльності у сфері інформаційної безпеки. Зокрема:

- Указ Президента України № 47/2017 «Про Доктрину інформаційної безпеки України» став фундаментальним документом, що визначив ключові напрями державної політики. У Доктрині наголошується на необхідності протидії інформаційним операціям, захисту національного інформаційного простору та формуванню позитивного міжнародного іміджу України [16]. Доктрина закріпила концептуальне уявлення про інформаційну політику як складову національної безпеки [1, с. 6–7];

- Указ Президента України № 44/2021 «Про Стратегію кібербезпеки України» розширив політико-правові механізми, інтегрувавши їх із цифровим виміром. У Стратегії визначено, що кібератаки, спрямовані на критичну інфраструктуру та медіа, є одним із головних елементів гібридної агресії. Документ акцентує на міжнародному співробітництві та взаємодії з НАТО й ЄС у сфері кіберзахисту [17];

- Указ Президента України № 106/2021 «Про створення Центру протидії дезінформації» започаткував новий інституційний механізм [18]. Центр виконує завдання з виявлення й нейтралізації дезінформаційних кампаній, координує роботу державних органів і співпрацює з міжнародними партнерами. Це свідчить про прагнення до інституціоналізації інформаційної політики.

- Стратегія національної безпеки України (2020 р.) також містить положення щодо інформаційної стійкості та протидії пропаганді [19]. Вона вперше на рівні стратегічного документу виокремила завдання інформаційної політики у сфері протидії гібридній війні.

Українські дослідники наголошують, що ці документи окреслили рамки, але їхня реалізація потребує комплексної міжвідомчої координації та інтеграції з європейськими практиками [3, с. 47-48]. Зарубіжні аналітики [6; 7] зазначають, що подібні стратегії в країнах Балтії та Польщі довели ефективність лише тоді, коли були підкріплені сталими інституційними механізмами, а не лише

політичними деклараціями.

Зазначимо, що сучасна інформаційна політика України формується не лише у внутрішньому політико-правовому полі, але й в умовах інтеграції до європейського та євроатлантичного простору. Це зумовлює потребу гармонізації українських нормативних актів із міжнародними документами. Так:

- Digital Services Act Європейського Союзу (2022) визначає обов'язки онлайн-платформ щодо контролю за поширенням незаконного та шкідливого контенту, прозорості алгоритмів та відповідальності за дезінформацію [20]. Для України його імплементація є ключовою, адже саме соціальні мережі та цифрові платформи стали головним каналом російських інформаційних атак\$

- European Democracy Action Plan (2020) спрямований на зміцнення демократичних інститутів, підтримку незалежних ЗМІ та розвиток медіаграмотності. Він акцентує на ролі правових механізмів у боротьбі з дезінформацією, що відповідає українським викликам [21];

- Кодекс практик проти дезінформації (2022, оновлений) створює рамкові механізми саморегуляції для цифрових платформ, забезпечуючи прозорість політичної реклами та співпрацю з дослідницькими інституціями [22]. Україна може використовувати цей документ як орієнтир у співпраці з глобальними ІТ-компаніями;

- NATO StratCom COE (зокрема аналітичні звіти 2016 та 2024 рр.) розробляє стандарти та рекомендації для країн-членів НАТО у сфері стратегічних комунікацій, протидії пропаганді та маніпуляціям [6; 7]. Українські інституції активно залучаються до цієї співпраці, адаптуючи національні механізми.

Як зазначають зарубіжні автори, правові та політичні інструменти міжнародних організацій дієві лише тоді, коли вони поєднані з розвитком критичного мислення та комунікаційної стійкості суспільства [5, р. 17]. Для України це означає, що інтеграція у правові стандарти ЄС має супроводжуватися розбудовою власної інституційної та нормативної бази.

Інституційна структура інформаційної політики України складається з низки органів, що виконують різні, але взаємопов'язані функції:

- Рада національної безпеки і оборони України (РНБО) координує й контролює діяльність у сфері інформаційної безпеки, ухвалює стратегічні рішення, які потім реалізуються на урядовому рівні;

- Міністерство культури та інформаційної політики України відповідає за формування державної політики у сфері медіа, інформаційної безпеки та міжнародної комунікації.

- Центр протидії дезінформації (створений 2021 р.) виконує роль аналітичного та координаційного органу, зосередженого на виявленні, аналізі та нейтралізації дезінформаційних кампаній;

- Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ) здійснює технічний та кіберзахист, який прямо впливає на інформаційну безпеку.

Однак, як підкреслює А. Антипова, проблема цих інституцій полягає у відсутності достатньої координації та дублюванні функцій, що знижує ефективність реагування на інформаційні загрози [3, с. 48].

Важливою особливістю української моделі інформаційної політики є значна роль громадянського суспільства та незалежних медіа. Після 2014 р. в Україні сформувалася розгалужена мережа громадських організацій, що спеціалізуються на фактчекінгу та протидії дезінформації (StopFake, VoxCheck). Незалежні журналістські ініціативи стали невід'ємним елементом інформаційної безпеки, доповнюючи державні інституції. Як зазначає О. Зернецька, саме партнерство держави з громадянським суспільством дозволяє досягати стійкості, адже державні механізми самі по собі є недостатніми [4, с. 218].

Таким чином, в умовах гібридної війни медіа та громадські ініціативи відіграють не лише роль «четвертої влади», але й функцію «інформаційного щита».

Україна активно інтегрується у систему міжнародних інституцій, що працюють у сфері стратегічних комунікацій і протидії дезінформації: NATO StratCom COE (Рига) – платформа для обміну досвідом і напрацювання стандартів у сфері стратегічних комунікацій. East StratCom Task Force (ЄС) – підтримує Україну у виявленні російських дезінформаційних кампаній. Співпраця з державами Балтії та Польщею – забезпечує трансфер успішних практик (зокрема, систем моніторингу інформаційних загроз та правових обмежень для ворожих медіа). Як зазначають А. Хоскінс та Б. О'Локлін, у сучасному світі боротьба з дезінформацією можлива лише на наддержавному рівні, оскільки інформаційні потоки не визнають державних кордонів [5, р. 18].

Загалом можна стверджувати, що інституційний вимір інформаційної політики України формується за змішаною моделлю: державні органи створюють правові рамки та інфраструктуру безпеки, тоді як громадянське суспільство та міжнародні партнери забезпечують гнучкість і динамічність реагування. Проблемою залишається недостатня координація між органами влади та обмежене фінансування. Проте взаємодія держави, медіа та міжнародних структур дозволяє Україні поступово формувати модель інформаційної стійкості, яка відповідає викликам гібридної війни.

Перспективи розвитку інформаційної політики України в умовах гібридної війни пов'язані з удосконаленням нормативної бази. Необхідно:

- забезпечити системність законодавства, усунути фрагментарність у сфері протидії дезінформації (Компанцева, 2017, с. 9);

- запровадити чіткі механізми відповідальності цифрових платформ за поширення шкідливого контенту відповідно до вимог DSA;

- адаптувати законодавство щодо інформаційної безпеки до стандартів ЄС і НАТО.

Для ефективної реалізації політики потрібне посилення інституційних можливостей: удосконалення координації між РНБО, Міністерством культури та інформаційної політики, Центром протидії дезінформації; створення єдиного оперативного координаційного центру, що об'єднає функції моніторингу, аналізу та реагування на інформаційні атаки; розширення кадрового потенціалу в сфері стратегічних комунікацій. Як зазначає Антипова, брак координації залишається однією з головних проблем української інформаційної політики [3, с. 50].

Ключовим завданням є формування інформаційної стійкості суспільства, а саме: підвищення медіаграмотності через інтеграцію освітніх програм; підтримка незалежних медіа та фактчекінгових ініціатив, які є ефективним інструментом боротьби з дезінформацією; посилення співпраці з громадянським суспільством як партнером держави у протидії гібридним загрозам (Зернецька, 2011, с. 218).

Україна повинна активно інтегруватися у європейський та євроатлантичний безпековий простір. Зокрема, це: співпраця з NATO StratCom COE для адаптації кращих практик стратегічних комунікацій; участь у програмах East StratCom Task Force ЄС та «EUvsDisinfo»; узгодження національних документів зі стратегічними ініціативами ЄС (EDAP, European Media Freedom Act). Як зазначають А. Хоскінс та Б. О'Локлін, лише інтеграція національної політики в міжнародні рамки дає змогу ефективно протидіяти глобальним інформаційним загрозам [5, р. 19].

Висновки. 1. Інформаційна політика є інтегрованим явищем, яке поєднує правові норми, інституційні практики та стратегічні комунікації. Вона формується у трикутнику понять «інформаційна політика – інформаційна безпека – гібридна війна».

2. Нормативно-правова база України включає Конституційні положення, базові закони («Про інформацію», «Про медіа», «Про національну безпеку»), а також стратегічні документи (Доктрина інформаційної безпеки 2017 р., Стратегія кібербезпеки 2021 р., створення Центру протидії дезінформації). Важливим є і процес адаптації до європейських стандартів (DSA, EDAP, Кодекс практик проти дезінформації).

3. Інституційно-організаційний вимір демонструє, що державні органи (РНБО, МКІП, ДССЗІ), громадянське суспільство та міжнародні партнери формують змішану модель інформаційної політики. Її сильними сторонами є партнерство з медіа та міжнародними структурами, а слабкими — дублювання функцій та недостатня координація.

4. Перспективи розвитку пов'язані з оптимізацією законодавства, посиленням інституційної спроможності, формуванням інформаційної стійкості суспільства та інтеграцією в європейські й євроатлантичні стандарти. Україна має перейти від реактивної моделі протидії до проактивної, заснованої на стійкості та партнерстві.

Загалом, політико-правові механізми інформаційної політики в умовах гібридної війни повинні функціонувати як система взаємодії права, інституцій та стратегічних комунікацій, що дозволить державі не лише протистояти загрозам, але й формувати власний позитивний інформаційний простір.

Бібліографічний список:

1. Компанцева Л. Доктрина інформаційної безпеки України: теоретико-правові засади. *Інформація і право*, Київ: Науково-дослідний інститут інформатики і права. 2017. № 3(22). С. 5–12.
2. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 72 p.
3. Антипова А. Стратегічні комунікації як складова інформаційної безпеки держави. *Юридичний часопис*

Національної академії внутрішніх справ. Київ: Національна академія внутрішніх справ. 2023. № 13(1). С. 44–52.

4. Зернецька О. Глобальний розвиток комунікацій: інформаційна політика та міжнародні відносини. Київ: Видавництво «Києво-Могилянська академія». 2011. 368 с.
5. Hoskins, A., & O'Loughlin, B. (2010). *War and media: The emergence of diffused war*. Cambridge: Polity Press, 225 p.
6. NATO Strategic Communications Centre of Excellence (StratCom COE). (2016). *Russian information campaign against Ukrainian state and defence forces: Framing of the Ukraine–Russia conflict in online and social media*. Riga: NATO StratCom COE, 108 p.
7. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). *War on all fronts: How the Kremlin's media ecosystem broadcasts the war in Ukraine*. Riga: NATO StratCom COE, 146 p.
8. McQuail, D. (2010). *McQuail's Mass Communication Theory* (6th ed.). London: Sage Publications, 621 p.
9. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*, № 31. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
10. Castells, M. (2009). *Communication power*. Oxford: Oxford University Press, 571 p.
11. Грищенко К. Гібридна війна: виклики та загрози для інформаційної безпеки України. *Науковий вісник Національного університету «Острозька академія»*. Серія «Політологія». Острог: НаУОА. 2020. № 2(12). С. 15–23.
12. Конституція України (1996, ред. 2024 р.). *Відомості Верховної Ради України*, № 30, ст. 141. URL: <https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80>
13. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII (ред. 2024 р.). *Відомості Верховної Ради України*, № 48. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
14. Закон України «Про медіа» від 13 грудня 2022 року № 2849-IX. *Відомості Верховної Ради України*, № 4, 2023. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>
15. Закон України «Про національну безпеку» від 21.06.2018 № 2469-VIII (чинна редакція станом на 21.08.2025). Офіційний портал Верховної Ради України. URL: <https://zakon.rada.gov.ua>
16. Указ Президента України № 47/2017 «Про Доктрину інформаційної безпеки України». *Офіційний вісник Президента України*. URL: <https://www.president.gov.ua/documents/472017-21374>
17. Указ Президента України № 44/2021 «Про Стратегію кібербезпеки України». *Офіційний вісник Президента України*. URL: <https://www.president.gov.ua/documents/442021-36441>
18. Указ Президента України № 106/2021 «Про створення Центру протидії дезінформації». *Офіційний вісник Президента України*. URL: <https://www.president.gov.ua/documents/1062021-37533>
19. Стратегія національної безпеки України. Указ Президента України від 14.09.2020 № 392/2020. URL: <https://zakon.rada.gov.ua/go/392/2020>
20. European Commission. (2022). *Digital Services Act: Regulation (EU) 2022/2065*. Brussels: Publications Office of the European Union, 152 p.
21. European Commission. (2020). *European Democracy Action Plan*. Brussels: Publications Office of the European Union, 24 p.
22. European Commission. (2022). *Code of Practice on Disinformation (Strengthened 2022)*. Brussels: Publications Office of the European Union, 32 p.

References:

1. Kompantseva, L. (2017). Doctrine of information security of Ukraine: Theoretical and legal foundations. *Information and Law*, No. 3(22), 5–12. Kyiv: Research Institute of Informatics and Law.
2. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 72 p.
3. Antypova, A. (2023). Strategic communications as a component of state information security. *Law Journal of the National Academy of Internal Affairs*, No. 13(1), 44–52. Kyiv: National Academy of Internal Affairs.
4. Zernetska, O. (2011). *Global Development of Communications: Information Policy and International Relations*. Kyiv: Kyiv-Mohyla Academy Publishing, 368 p.
5. Hoskins, A., & O'Loughlin, B. (2010). *War and Media: The Emergence of Diffused War*. Cambridge: Polity Press, 225 p.
6. NATO Strategic Communications Centre of Excellence (StratCom COE). (2016). *Russian information campaign against Ukrainian state and defence forces: Framing of the Ukraine–Russia conflict in online and social media*. Riga: NATO StratCom COE, 108 p.
7. NATO Strategic Communications Centre of Excellence (StratCom COE). (2024). *War on all fronts: How the Kremlin's media ecosystem broadcasts the war in Ukraine*. Riga: NATO StratCom COE, 146 p.
8. McQuail, D. (2010). *McQuail's Mass Communication Theory* (6th ed.). London: Sage Publications, 621 p.
9. Verkhovna Rada of Ukraine. (2018). Law of Ukraine “On National Security of Ukraine” of June 21, 2018 No. 2469-VIII. *Vidomosti Verkhovnoi Rady Ukrainy*, No. 31.

URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

10. Castells, M. (2009). *Communication Power*. Oxford: Oxford University Press, 571 p.
11. Hryshchenko, K. (2020). Hybrid war: Challenges and threats to the information security of Ukraine. *Scientific Bulletin of the National University "Ostroh Academy". Series "Political Science"*, No. 2(12), 15–23. Ostroh: NaUOA.
12. Constitution of Ukraine. (1996, as amended 2024). *Vidomosti Verkhovnoi Rady Ukrainy*, No. 30, Art. 141. URL: <https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80>
13. Verkhovna Rada of Ukraine. (1992/2024). Law of Ukraine "On Information" of October 2, 1992 No. 2657-XII (as amended 2024). *Vidomosti Verkhovnoi Rady Ukrainy*, No. 48. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
14. Verkhovna Rada of Ukraine. (2022/2023). Law of Ukraine "On Media" of December 13, 2022 No. 2849-IX. *Vidomosti Verkhovnoi Rady Ukrainy*, No. 4. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>
15. Verkhovna Rada of Ukraine. (2018/2025). Law of Ukraine "On National Security of Ukraine" of June 21, 2018 No. 2469-VIII (current edition as of 21.08.2025). *Official Portal of the Verkhovna Rada of Ukraine*. URL: <https://zakon.rada.gov.ua>
16. President of Ukraine. (2017). Decree No. 47/2017 "On the Doctrine of Information Security of Ukraine". *Official Bulletin of the President of Ukraine*. URL: <https://www.president.gov.ua/documents/472017-21374>
17. President of Ukraine. (2021). Decree No. 44/2021 "On the Cybersecurity Strategy of Ukraine". *Official Bulletin of the President of Ukraine*. URL: <https://www.president.gov.ua/documents/442021-36441>
18. President of Ukraine. (2021). Decree No. 106/2021 "On the establishment of the Centre for Countering Disinformation". *Official Bulletin of the President of Ukraine*. URL: <https://www.president.gov.ua/documents/1062021-37533>
19. President of Ukraine. (2020). *National Security Strategy of Ukraine*. Decree No. 392/2020 of September 14, 2020. URL: <https://zakon.rada.gov.ua/go/392/2020>
20. European Commission. (2022). *Digital Services Act: Regulation (EU) 2022/2065*. Brussels: Publications Office of the European Union, 152 p.
21. European Commission. (2020). *European Democracy Action Plan*. Brussels: Publications Office of the European Union, 24 p.
22. European Commission. (2022). *Code of Practice on Disinformation (Strengthened 2022)*. Brussels: Publications Office of the European Union, 32 p.

Pashkovskiy V. Identification of political and legal mechanisms of state information security under hybrid warfare

The article provides a comprehensive study of the political and legal mechanisms of the state's information policy under the conditions of hybrid warfare. It is demonstrated that Ukraine's information policy develops through the combination of legal norms, strategic documents, and institutional practices aimed at countering information threats. The study: identified the key theoretical and conceptual foundations of information policy and its correlation with the categories of information security and hybrid warfare; analyzed Ukraine's legal and regulatory framework (Constitution, laws, presidential decrees, strategies) as well as international standards (DSA, EDAP, Code of Practice on Disinformation, NATO StratCom COE and EU documents); defined institutional and organizational mechanisms, including the activities of the NSDC, the Ministry of Culture and Information Policy, the Centre for Countering Disinformation, as well as the role of civil society and international partners; systematized political and legal instruments: "hard" (sanctions, blocking of resources, media regulation) and "soft" (strategic communications, information campaigns, fact-checking initiatives); formulated perspectives and recommendations for improving information policy: harmonization of legislation with European standards, creation of a unified coordination structure, development of societal resilience, and integration into the Euro-Atlantic security space. It is concluded that the effectiveness of the state's information policy in countering hybrid threats is possible only through the synergy of political and legal norms, institutional coordination, and strategic communications. In general, political and legal mechanisms of information policy in the context of hybrid warfare should function as a system of interaction between law, institutions, and strategic communications, which will allow the state not only to resist threats, but also to form its own positive information space.

Keywords: *information policy, political and legal mechanisms, hybrid warfare, information security, strategic communications, disinformation, legal regulation.*