Інформаційне право

УДК 351.862:355.41:004.056(477)

DOI https://doi.org/10.5281/zenodo.17757320

Державна політика інформаційної безпеки в умовах гібридних загроз

Бідзіля Юрій Михайлович,
доктор наук із соціальних комунікацій, професор кафедри журналістики, декан філологічного факультету, Державний вищий навчальний заклад «Ужгородський національний університет», м. Ужгород, Україна, https://orcid.org/0000-0001-5134-3239

Прийнято: 10.11.2025 | Опубліковано: 29.11.2025

Анотація. Актуальність дослідження зумовлено зростанням масштабів і складності гібридних загроз, що спрямовані проти державних інституцій, суспільства та критичної інформаційної інфраструктури України. Метою дослідження є теоретичне обґрунтування системних засад формування державної політики інформаційної безпеки України та розроблення моделі стратегічного управління в умовах гібридних загроз з урахуванням чинників медіасередовища, цифрової дипломатії, кіберзахисту та суспільної стійкості. Методологічну основу складають системна й структурно-функціональна практики, методи стратегічного та порівняльного аналізу, інституційного моделювання, ризикоорієнтованого оцінювання, контент-аналізу та формалізовані методи індикативного прогнозування. Застосовано елементи статистичного порівняння міжнародних індексів кіберготовності та цифрового розвитку. Отримані результати підтверджують сформованість базових спроможностей України у сфері інформаційної та кібербезпеки,

охоплюючи розвиток цифрової інфраструктури, інституцій STRATCOM, системи реагування на кібератаки й механізмів протидії дезінформації. Водночас виявлено низку структурних викликів: нерівномірність розвитку мережевої інфраструктури, недостатня глибина впровадження протоколів DNSSEC та IPv6, обмеженість кадрових ресурсів та потреба у підвищенні медіа- й цифрової грамотності населення. Обґрунтовано багаторівневу модель інформаційної стійкості «держава – суспільство – інфраструктура» та запропоновано поетапний алгоритм розроблення комплексної стратегії інформаційної безпеки, що містить діагностику загроз, стратегічне планування, нормативно-правове забезпечення, інституційне зміцнення, цифрову модернізацію та міжнародну кооперацію. Перспективи подальших досліджень полягають у розробленні національної матриці ризиків інформаційного середовища, інструментарію оцінювання суспільної медіастійкості, моделюванні загроз на основі даних OSINT і SIGINT, зокрема побудові механізмів інтеграції міжнародних стандартів кіберзахисту у практику українського державного управління.

Ключові слова: стратегічні комунікації, цифровий суверенітет, кіберстійкість, дезінформація, інформаційна політика, суспільна стійкість, цифрова дипломатія, національна безпека.

State policy of information security under hybrid threats

Yuriy Bidzilya,
Doctor of Science in Social Communications, Professor of the Department of Journalism, Dean of the Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine, https://orcid.org/0000-0001-5134-3239

Abstract. The relevance of this study is driven by the escalating scale and complexity of hybrid threats that systematically target state institutions, society, and

Ukraine's critical information infrastructure. The purpose of the research is to theoretically substantiate the systemic foundations of forming Ukraine's state information security policy and to develop a model of strategic governance under hybrid threats, taking into account media ecosystem factors, digital diplomacy, cyber defence, and societal resilience. The methodological framework encompasses systemic and structural-functional approaches, methods of strategic and comparative analysis, institutional modeling, risk-oriented assessment, content analysis, and formalized indicative forecasting techniques. The research also uses statistical comparisons of international cyber-readiness and digital development indices. The results confirm the development of Ukraine's core capabilities in information and cybersecurity, including digital infrastructure, STRATCOM institutions, cyber incident response mechanisms, and instruments to counter disinformation. At the same time, several structural challenges were identified, including uneven development of network infrastructure, insufficient deployment of DNSSEC and IPv6, limited human resources, and a need to strengthen media and digital literacy. A multi-level «state – society – infrastructure» information resilience model is substantiated, and a phased algorithm for developing a comprehensive information security strategy is proposed, encompassing threat diagnostics, strategic planning, regulatory support, institutional strengthening, digital modernisation, and international cooperation. Future research prospects include developing a national information threat matrix, tools for assessing societal media resilience, modelling hybrid threats using OSINT- and SIGINT-based approaches, and designing mechanisms to integrate international cybersecurity standards into Ukrainian public governance practice.

Keywords: strategic communications, digital sovereignty, cyber resilience, disinformation, information policy, societal resilience, digital diplomacy, national security.

Постановка проблеми. Сучасна епоха характеризується

трансформацією конфліктів із переважно військових у комплексні гібридні протистояння, де інформаційний простір є стратегічним інструментом боротьби за політичний вплив, суспільну свідомість і державний суверенітет. Для України питання інформаційної безпеки має екзистенційний характер, оскільки країна перебуває в умовах масштабної збройної агресії та систематичного інформаційно-психологічного тиску з боку держави-агресора [1, с. 115]. Дезінформація, кібератаки, маніпулювання громадською думкою, спроби підриву демократичних інститутів і стратегічних комунікацій формують нову конфігурацію загроз, що потребує проактивної, науково обґрунтованої та стратегічно узгодженої державної політики [2, p. 251].

У цих умовах важливим є переосмислення ролі інформаційної безпеки як базового елементу національної безпеки, засобу захисту державності, інструменту підтримки суспільної стійкості та чинника міжнародної суб'єктності України. Зростання складності кіберсередовища, цифровізація державного управління, медіатизація соціальних процесів і посилення інформаційної конкуренції вимагають розроблення інтегрованої моделі інформаційної політики, здатної забезпечити технологічну, інституційну та комунікаційну стійкість держави [3, p. 20]. З огляду на це комплексне дослідження стратегічних засад інформаційної безпеки є найактуальнішим у контексті повоєнного відновлення, євроатлантичної інтеграції та побудови стійкої демократичної системи.

Аналіз останніх досліджень і публікацій. Сучасні наукові засади інформаційної та кібербезпеки трансформуються від суто технічних рішень на користь комплексних моделей, де визначальними є державна політика, цифровий суверенітет та здатність суспільства протидіяти гібридним впливам. Зокрема, дослідник Ґ. Деде зі співавторами (G. Dede et al.) [4] доводять, що кіберстійкість є базовою умовою розвитку IoT-інфраструктури й досягнення Цілей сталого розвитку. У контексті організаційної адаптації вчений С. Махмуд зі співавторами (S. Mahmood et al.) [5] підкреслюють роль навчання

 ISSN: 3041-2110

та гнучких управлінських практик у протидії кризовим кіберзагрозам, зокрема у вищій освіті, тоді як автори С. Муштак і М. Шах (S. Mushtaq & M. Shah) [6] визначають необхідність інтеграції технічних, управлінських і поведінкових інструментів для протидії кіберзлочинності в е-урядуванні. На технологічному рівні науковець Ф. Генуаріо зі співавторами (F. Genuario et al.) [7] демонструють ефективність глибинного навчання й ансамблевих моделей для раннього виявлення атак, а дослідник С. Зохайб зі співавторами (S. Zohaib et al.) [8] обґрунтовують переваги Zero Trust VPN у гібридних робочих середовищах. Водночас цифрова трансформація інструментів контролю охоплює не лише сферу кіберзахисту, а й механізми протидії економічним злочинам та розслідування кримінальних правопорушень. Так, вчений Х. Аль-Абабне зі співавторами (H. Al-Ababneh et al.) [9] визначають, що використання Big Data, блокчейну та відкритих даних істотно підвищує ефективність виявлення економічних злочинів у сфері публічних закупівель, забезпечуючи вищу прозорість, точність контролю та зменшення корупційних ризиків. Доповнюючи цю практику, науковець І. Демидов зі співавторами (I. Demidov et al.) [10] доводять, що застосування лазерного 3D-сканування значно підвищує точність реконструкції деталей особливо тяжких злочинів, забезпечуючи наукову верифікацію слідчих версій і відтворення динаміки подій із високим рівнем доказовості. Автор Д. Мюгге (D. Mügge) [11] розглядає європейську стратегію штучного інтелекту як баланс між автономією, конкуренцією та правами людини, а дослідник П. Свайр зі співавторами (P. Swire et al.) [12] наголошують, що надмірна локалізація даних може послаблювати кібербезпеку через затримки доступу до критичної інформації. Водночас науковець Т. Тропіна (T. Tropina) [13] акцентує на ризику зниження стандартів прав людини у глобальних угодах про кіберзлочинність. Зокрема, автори Дж. Бергауст і С. Селлеваг (J. Bergaust & S. Sellevåg) [14] розглядають багатовимірність гібридних впливів нижче порогу війни, а дослідник Дж. Тумфарт (J. Thumfart) [15] зазначає

ISSN: 3041-2110

необхідність юридичного захисту права на цифровий доступ. Учений С.-Д. Бахманн зі співавторами (S.-D. Bachmann) [16], аналізуючи російську агресію проти України, підтверджують вирішальну роль дезінформації та інформаційних операцій у гібридній війні та потребу комплексної багаторівневої протидії.

Узагальнення цих досліджень демонструє системний перехід до інтегрованої моделі інформаційної безпеки, що об'єднує технологічні, правові, дипломатичні та соціально-комунікаційні інструменти. Центральними є цифровий суверенітет, суспільна стійкість до інформаційних впливів, міжнародна співпраця й дотримання прав людини – напрями, що формують стратегічну рамку трансформації політики України в умовах гібридної війни.

Виділення невирішених раніше частин загальної проблеми. Попри наявні дослідження, низка аспектів інформаційної безпеки залишається нерозв'язаною, зокрема питання поєднання цифрового суверенітету з правами людини, формування вимірюваних показників медіастійкості суспільства та узгодження державних і громадянських механізмів протидії гібридним загрозам. Водночас наявні проблеми інституційної координації, оцінювання ризиків інформаційного впливу та розбудови цифрової інфраструктури з урахуванням воєнних умов. Дослідження спрямоване на розроблення інтегрованої моделі державної політики інформаційної безпеки, що поєднує стратегічні комунікації, кібероборону та суспільну стійкість та визначення системи індикаторів для оцінювання ефективності інформаційної стратегії України. Практична цінність роботи полягає у можливості використання запропонованих практик для підвищення інформаційної стійкості держави, вдосконалення нормативного забезпечення, зміцнення системи стратегічних комунікацій і формування інструментів протидії дезінформації в умовах воєнного стану.

Формулювання цілей статті (визначення завдання). Метою

ISSN: 3041-2110

дослідження є обґрунтування теоретичних засад і практичних механізмів формування державної політики інформаційної безпеки України в умовах гібридних загроз з урахуванням трансформації стратегічних комунікацій, цифрової дипломатії, механізмів кіберзахисту, розвитку інформаційної інфраструктури та формування суспільної інформаційної стійкості.

Виклад основного матеріалу дослідження. Інформаційна безпека у сучасному державному управлінні розглядається як базова умова суверенітету та стійкості держави. Вона охоплює захист інформаційних ресурсів, надійність комунікацій, безперебійність цифрової інфраструктури та формування суспільної здатності протидіяти маніпуляціям. У наукових дослідженнях інформаційна безпека трактується як взаємодія трьох вимірів [1; 7; 17]: технологічного (захист систем і мереж), комунікаційного (стабільність медіасередовища) та соціально-політичного (інституційна стійкість держави й суспільства). Сучасні загрози формуються в умовах гібридної війни та містять інформаційно-психологічні операції, дезінформацію та кібератаки на критичну інфраструктуру. Вони спрямовані на підрив довіри, дестабілізацію політичних процесів і трансформацію громадської думки. Однак кіберкомпонент є лише одним із вимірів: визначальною умовою стійкості є інституційна здатність держави забезпечувати стратегічну комунікацію, інформаційну стабільність та ефективне управління інформаційним простором [12; 17]. У цьому контексті інформаційна політика є не лише технічним інструментом захисту цифрових систем, а й інституційним механізмом формування стійкого інформаційного середовища. До її основних завдань належать: розвиток стратегічних комунікацій, підтримка незалежних медіа, створення національної цифрової екосистеми та підвищення цифрової грамотності населення.

Перехід до інституційного виміру є значущим для України, де сформовано багаторівневу систему нормативно-правового регулювання та організаційного забезпечення, спрямовану на протидію гібридним загрозам і

ISSN: 3041-2110

зміцнення інформаційного суверенітету. Основним законодавчим документом є Закон України «Про національну безпеку України» [18], що визначає інформаційну безпеку одним з базових елементів національної політики та формує модель сектору безпеки та оборони, до складу якого належать суб'єкти забезпечення кібер- та інформаційної стійкості. Спеціальне правове підґрунтя створює Доктрина інформаційної безпеки України [19], що окреслює стратегічні цілі, принципи та напрями підтримання інформаційної стійкості держави, формування інформаційної культури, протидії інформаційним операціям та дезінформації. Комплементарними документами є Стратегія національної безпеки України [20], Стратегія кібербезпеки України [21] та рішення Ради національної безпеки і оборони, що спрямовані на захист інформаційного простору, санкційний тиск на пропагандистські ресурси та формування архітектури кіберзахисту. У сфері медіа та цифрових комунікацій чільне місце посідають Закони України «Про медіа» [22] та «Про основні засади забезпечення кібербезпеки України» [23], що регулюють функціонування медійного середовища, діяльність онлайн-платформ, механізми реагування на кіберінциденти та взаємодію держави з приватним сектором.

Інституційна система гарантування інформаційної безпеки є багатокомпонентною й координаційною установою. Провідну роль відіграє Рада національної безпеки і оборони України, що формує стратегічні рішення та координує діяльність сил безпеки. Центральним оперативним органом є Служба безпеки України, уповноважена здійснювати контррозвідувальні заходи у сфері інформаційної та кібербезпеки.

Водночас важливу роль у формуванні стійкості відіграють й інститути політичної комунікації та публічної дипломатії, зокрема Міністерство закордонних справ України, що реалізує стратегію цифрової дипломатії, та Міністерство культури та інформаційної політики, відповідальне за державну інформаційну політику і розвиток медіасередовища. Партнерську підтримку

забезпечують громадські організації, аналітичні центри та незалежні медіа як елемент демократичної інформаційної безпеки.

Таким чином, нормативно-правова та інституційна системи України формують комплексну архітектуру реагування на сучасні гібридні загрози, поєднуючи механізми державного управління, військової та цифрової оборони, стратегічних комунікацій і суспільної стійкості. Однак ефективність цієї системи не може оцінюватися виключно на основі правових та організаційних положень. Необхідним є емпіричний аналіз реальних спроможностей держави щодо гарантування інформаційної безпеки, що передбачає застосування оцінювальної практики й порівняльних аналітичних інструментів.

З цією метою доцільно розробити узагальнену матрицю показників кібер- та інформаційної безпеки України, що відображає базові стратегічні, превентивні та адаптивні параметри сформованої системи безпекових спроможностей держави та дає змогу оцінити рівень її функціональної готовності в умовах гібридної агресії (табл. 1). Застосування таких індикаторів забезпечує комплексне розуміння стану інформаційної стійкості, враховуючи не лише нормативні засади, а й фактичні характеристики захисту критичної інфраструктури, наявності кіберкомандування, механізмів реагування на інциденти, інформаційної протидії та стратегічних комунікацій.

Таблиця 1

Матриця показників кібер- та інформаційної безпеки України в умовах гібридних загроз

Показник	Макс. бал	Факт. бал	% виконання	Значення для інфобезпеки
Стратегічні індикатори				
Політика кібербезпеки	15	15	100%	Наявність стратегічних документів, програм, доктрин
Глобальний внесок у кібербезпеку	6	4	67%	Участь у міжнародних коаліціях, CERT/CSIRT, співпраця з НАТО, ЄС
Освіта та професійний розвиток	10	10	100%	Підготовка кадрів, кіберосвіта, програми НУО та держави
Дослідження і	4	4	100%	Інновації, наука, R&D у сфері

ISSN: 3041-2110

Показник	Макс. бал	Факт. бал	% виконання	Значення для інфобезпеки
розробки				кібер- та інформаційної безпеки
Превентивні індикатори				
Захист критичної інформаційної інфраструктури	12	12	100%	Стійкість енергетики, транспорту, телекомунікацій до атак
Кібербезпека цифрових сервісів	12	12	100%	Захист державних цифрових платформ (Дія, реєстри)
Аналіз загроз і підвищення обізнаності	12	9	75%	Система моніторингу, STRATCOM, медіаграмотність суспільства
Захист персональних даних	4	4	100%	Законодавство, відповідність GDPR, держстандарти
Адаптивні індикатори				
Реагування на кіберінциденти	14	9	64%	Швидкість реагування CERT-UA, СБУ, приватних структур
Управління кіберкризами	9	5	56%	Наявність кризових протоколів, національний SOC, кіберрезерви
Боротьба з кіберзлочинністю	16	16	100%	Робота кіберполіції, прокуратури, міжнародні справи
Військова кібероборона	6	6	100%	Захист військових систем, взаємодія з союзниками, кіберкомандування

Джерело: сформовано автором на підставі [24; 25]

Високі значення стратегічних і превентивних показників засвідчують сформованість базових елементів інформаційної безпеки, зокрема наявність національних доктрин, кіберзаконодавства, інституцій STRATCOM та розвиненої інфраструктури кіберзахисту. Водночас нижчі результати у сфері кризового реагування та оперативної взаємодії цифрових систем вказують на потребу подальшого посилення механізмів швидкого реагування на кібератаки, здатності до масштабованої протидії інформаційним операціям та розбудови системи кризових комунікацій.

Подальший аналіз ґрунтується на зіставленні національних характеристик з рейтингами провідних країн, що сприяє оцінюванню конкурентоспроможність України у сфері інформаційної та цифрової безпеки в динаміці геополітичного протистояння та цифрової трансформації (табл. 2).

ISSN: 3041-2110

Таблиця 2

Порівняння рівня кібербезпеки та цифрового розвитку

(станом на 30.09.2025 р.)

Місце в рейтингу	Країна	Національний індекс кібербезпеки	Рівень цифрового розвитку	Різниця	Інтерпретація
1	Бельгія	94,81	74,07	+20,74	Висока кіберготовність, розвинені цифрові сервіси
2	Естонія	93,51	75,59	+17,92	Світовий лідер у цифровому урядуванні та кіберстійкості
3	Чехія	90,91	69,21	+21,70	Сильні інституції та кіберкомандування
4	Німеччина	90,91	80,01	+10,90	Потужна цифрова інфраструктура, кібербезпека ЄС
5	Польща	87,01	65,03	+21,98	Динамічний розвиток кіберсектору, наближена до України модель
24	Україна	75,32	55,96	+19,36	Висока кіберстійкість в умовах воєнного стану, активна цифровізація

Джерело: сформовано автором на підставі [24; 25]

Отже, Україна посідає 24-те місце у світовому рейтингу кіберготовності, демонструючи результати, зіставні з країнами Центрально-Східної Європи та водночас поступаючись цифровим лідерам ЄС. Держави, що очолюють рейтинг – Бельгія, Естонія, Чехія, Німеччина, Польща – вирізняються високою синергією між кіберзахистом, інноваційністю цифрової інфраструктури та розвиненими інституційними механізмами стратегічних комунікацій. На цьому тлі Україна виявляє стале зміцнення кіберстійкості та розвиток цифрового сектору, що є визначальним в умовах воєнної агресії та масштабованого тиску на державні інформаційні системи. Показник різниці між рівнем кібербезпеки та цифрового розвитку засвідчує наявність потенціалу для подальшого технологічного зростання, зокрема у сфері модернізації цифрової інфраструктури, розвитку швидкісних мереж та впровадження сучасних протоколів безпеки. Досягнутий рівень кіберготовності України варто розглядати з урахуванням складних зовнішніх

умов, що підвищує значущість отриманих результатів та окреслює перспективні напрями поглиблення інформаційної стійкості.

Подальший аналіз цифрової інфраструктури й параметрів інтернет-екосистеми дасть змогу деталізувати сильні та вразливі компоненти національної інформаційної безпеки та визначити ресурси для її довгострокового зміцнення. Зокрема, важливо враховувати рівень розвитку мережевої архітектури, доступність широкосмугового інтернету, ступінь локалізації контенту, інтенсивність кіберінцидентів і готовність до відновлення цифрових сервісів (табл. 3).

Таблиця 3

Базові індикатори цифрової та інформаційної стійкості України, 2025 р.

Показник	**Значення для України**	**Середнє значення в Європі / ціль**	**Інтерпретація**
Позиція у світовому рейтингу кібербезпеки	24-те місце	-	Висока кіберготовність в умовах воєнного стану
Доступ до Інтернету населення	79%	90%	Високе проникнення, але нижче європейського рівня
4G покриття	96%	~98%	Майже повне покриття, критично важливо під час воєнних дій
5G доступність	< 1%	активно впроваджується в ЄС	Початкова стадія розвитку
Локально кешований контент	63%	Ціль 50% (Європа ~73%)	Пріоритетна ціль Internet Society, високий рівень контентної стійкості
Центри оброблення даних (Data Centers)	56	-	Значна внутрішня інфраструктура зберігання
Пункти обміну трафіком (IXP)	20 (86% мереж під'єднано)	Європа ~7	Висока децентралізація та автономність мереж
Впровадження IPv6	11%	32%	Потребує прискорення для майбутньої цифрової стійкості
Кіберінциденти (жовтень 2025)	1 випадок	-	Мінімальний рівень зафіксованих критичних інцидентів

ISSN: 3041-2110

Показник	Значення для України	Середнє значення в Європі / ціль	Інтерпретація
DNSSEC (захист доменів .ua)	<1% доменів	10%	Низький захист; зона покращення
RPKI IPv4 захищені префікси	68%	-	Достатній рівень маршрутизаційної безпеки
RPKI IPv6 захищені префікси	100%	-	Максимальний рівень безпеки IPv6-префіксів

Джерело: сформовано автором на підставі [25]

Аналіз показників доводить, що Україна має вагомі переваги у сфері цифрової оборони: розгалужена та децентралізована мережа (20 IXP, під'єднання 86% мереж), розвинена інфраструктура дата-центрів, широке покриття 4G та значний обсяг кешованого контенту. Це формує високу інтернет-стійкість, забезпечує швидке відновлення критичних сервісів і зменшує залежність від зовнішніх систем. Крім того, значний обсяг захищених IPv6-префіксів і використання RPKI підтверджують зрілість мережевої безпеки. Водночас наявні й уразливості: повільне впровадження IPv6 серед користувачів, відсутність широкого доступу до 5G, низький рівень DNSSEC-захисту доменів *.ua* та цифровий розрив між містом і селом. Це може стримувати масштабування цифрової інфраструктури, оскільки розрив між рівнем цифрового розвитку та кіберготовністю створює додаткові ризики для стабільності інформаційного середовища. У таких умовах зростання складності кібератак і інформаційних операцій вимагає не лише модернізації технічних систем, а й посилення кризових комунікацій, швидкого реагування на інциденти та підвищення цифрової грамотності населення.

Тож, загалом Україна демонструє значний потенціал цифрової оборони, поєднуючи високий рівень технологічної стійкості з потребою системного оновлення інфраструктури та механізмів управління. Подальший прогрес вимагає переходу від переважно реактивних заходів до проактивної моделі інформаційної безпеки, здатної забезпечити стійкість держави в умовах посилення гібридних загроз і глобальної цифрової конкуренції. Ефективна

стратегія має ґрунтуватися на принципах демократичної комунікації, цифрового суверенітету, технологічної незалежності, відкритості та інноваційності. Її основними пріоритетами є захист громадян і державності, прозорість інформаційних процесів, дотримання прав людини, розвиток кібероборони й інформаційної інфраструктури, формування культури цифрової безпеки та зміцнення національних механізмів протидії дезінформації. Концептуальною засадою визначено триєдину модель «держава – суспільство – інфраструктура», що забезпечує взаємодію стратегічних рішень, громадянської стійкості та технологічної основи захисту інформаційного простору (табл. 4).

Таблиця 4

Етапи формування комплексної інформаційної стратегії України

Назва етапу	Основний зміст	Основні завдання	Очікуваний результат
Діагностика та оцінювання загроз	Аналіз стану інформаційної та кібербезпеки	Оцінювання ризиків і гібридних загроз; виявлення критичних вразливостей; аудит чинної системи ІБ	Карта загроз та аналітична основа для планування
Стратегічне формування цілей і принципів	Визначення стратегічної моделі	Формування цілей і пріоритетів; закладення принципів ІБ; уточнення національних орієнтирів	Єдина стратегічна модель та місія
Інституційне дизайнування	Створення системи управління	Розподіл повноважень між органами; розвиток STRATCOM, CERT-UA, кіберкомандування; міжвідомчі механізми	Координована інституційна система
Нормативно-правове забезпечення	Модернізація законодавства	Оновлення законів і стандартів кіберзахисту; регламентація протидії дезінформації; стандарти реагування	Сучасна нормативна основа стійкості
Інфраструктурне посилення	Розвиток цифрової та мережевої інфраструктури	5G, дата-центри, IXP; DNSSEC, RPKI, IPv6; захист критичної інфраструктури	Технологічно стійка інфраструктура
Суспільна інформаційна стійкість	Розвиток людського капіталу та медіастійкості	Освіта і медіаграмотність; підтримка незалежних медіа; навчання держслужбовців	Стійке до дезінформації суспільство
Міжнародна координація та	Інтеграція у світові	Співпраця з НАТО, ЄС; цифрова дипломатія; спільні тренування	Підсилена міжнародна

ISSN: 3041-2110

Назва етапу	Основний зміст	Основні завдання	Очікуваний результат
дипломатія	безпекові системи		підтримка і коаліції
Моніторинг та адаптація	Циклічне оновлення стратегії	Критерії оцінювання (KPI); реакція на нові загрози; аудит ефективності	Гнучкість і адаптивність системи ІБ

Джерело: розроблено автором

Послідовна реалізація цих етапів забезпечує розвиток чотирьох основних напрямів: кібероборони, стійкого медійного середовища, інформаційної дипломатії та освітньо-комунікаційного складника. Кібероборона охоплює модернізацію систем виявлення та реагування на загрози, розвиток військово-цифрових спроможностей та міжнародну кооперацію. Медійний вимір передбачає підтримку незалежних ЗМІ, протидію інформаційним операціям і впровадження сучасних механізмів верифікації контенту. Інформаційна дипломатія сприяє формуванню стійкого міжнародного проукраїнського наративу та зміцненню цифрової присутності на глобальному рівні. Освітній компонент зосереджується на розвитку цифрової та медіаграмотності, підготовці фахівців у сфері кібербезпеки та стратегічних комунікацій. Таким чином, розроблена модель забезпечує перехід від фрагментарних заходів до системної та узгодженої інформаційної політики, що зміцнює здатність держави протистояти гібридним загрозам і формує підґрунтя для довгострокової стійкості та цифрового суверенітету України.

Висновки. Під час дослідження доведено, що інформаційна безпека формує ядро національної стійкості України в умовах гібридної агресії. Аналіз нормативної бази, інституційної архітектури та цифрової інфраструктури засвідчив наявність фундаментальної моделі кібер- та інформаційної оборони, здатної забезпечити базову захищеність держави й суспільства від зовнішніх інформаційних впливів. Порівняльний аналіз з провідними країнами ЄС продемонстрував, що попри відчутний розрив у рівні цифрового розвитку, Україна сформувала стійкі механізми функціонування цифрових сервісів,

ISSN: 3041-2110

підтримання мережевої інфраструктури та реагування на кібератаки, що є вагомим результатом у контексті воєнного тиску. Висока мобільність цифрової інфраструктури, розгалужена система обміну трафіком та оперативність стратегічних комунікацій забезпечують збереження функціональності державних сервісів і підтримують інституційну стійкість інформаційного простору. Водночас виявлено основні виклики: нерівномірність цифрового розвитку територій, недостатнє впровадження сучасних протоколів безпеки, обмежений розвиток 5G та потреба у зміцненні кадрового потенціалу. Запропонована трикомпонентна модель «держава – суспільство – інфраструктура» та поетапна практика стратегічного розвитку підтверджують необхідність синергетичного бачення інформаційної безпеки. Пріоритетами мають бути модернізація системи кібероборони, зміцнення комунікаційної інфраструктури, розвиток медіастійкості громадян, підтримка стратегічних комунікацій і посилення інформаційної дипломатії. Стратегічна мета полягає у переході від оборонно-реактивної до проактивної моделі інформаційної безпеки, що інтегрує технологічні, інституційні й суспільні механізми. Такі засади забезпечують не лише протидію загрозам, а й створення основи для демократичного розвитку, економічної стійкості та зміцнення міжнародної суб'єктності України.

Подальші дослідження можуть бути спрямовані на побудову національної матриці ризиків інформаційного середовища, кількісне моделювання показників інформаційної стійкості та порівняльний аналіз моделей STRATCOM у євроатлантичному просторі.

Список використаних джерел

1. Пашковський В. Ф. Ідентифікація політико-правових механізмів інформаційної безпеки держави в умовах гібридної війни. *Політичне життя.* 2025. № 3. С. 114–120. DOI: https://doi.org/10.31558/2519-2949.2025.3.15.

2. Bidzilya Yu. M., Solomin Ye. O., Shapovalova H. V., Georgiievska V. V.,

Poplavska N. M. The stability of State information in the face of terrorist threats. *Cuestiones Políticas*. 2021. Vol. 39, № 70. P. 250–269. DOI: https://doi.org/10.46398/cuestpol.3970.16.

3. Swire P., Kennedy-Mayo D., Bagley D., Krasser S., Modak A., Bausewein C. Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*. 2024. Vol. 9, № 1. P. 20–51. https://doi.org/10.1080/23738871.2024.2384724.

4. Dede G., Petsa A. M., Kavalaris S., Serrelis E., Evangelatos S., Oikonomidis I., Kamalakis T. Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. *Information.* 2024. Vol. 15, № 12. 798. DOI: https://doi.org/10.3390/info15120798.

5. Mahmood S., Chadhar M., Firmin S. Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. *Information.* 2024. Vol. 15, № 2. 106. DOI: https://doi.org/10.3390/info15020106.

6. Mushtaq S., Shah M. Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. *Information.* 2024. Vol. 15, № 10. 619. DOI: https://doi.org/10.3390/info15100619.

7. Genuario F., Santoro G., Giliberti M., Bello S., Zazzera E., Impedovo D. Machine learning-based methodologies for cyber-attacks and network traffic monitoring: A review and insights. *Information*. 2024. Vol. 15, № 11. 741. DOI: https://doi.org/10.3390/info15110741.

8. Zohaib S. M., Sajjad S. M., Iqbal Z., Yousaf M., Haseeb M., Muhammad Z. Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. *Information*. 2024. Vol. 15, № 11. 734. DOI: https://doi.org/10.3390/info15110734.

9. Al-Ababneh H. A., Fedorchuk Ya., Tymchyshyn A., Pishchenko H., Hrytsai S. The use of Big Data in the detection of economic crimes in public

procurements. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102, № 24. P. 8860–8876. URL: https://www.jatit.org/volumes/Vol102No24/3Vol102No24.pdf (дата звернення: 01.09.2025).

10. Demidov I., Tymchyshyn A., Filashkin V., Pavlenko S., Sevruk V. Investigation of especially grave crimes using laser scanning technology to reproduce the dynamics of events. *WSEAS Transactions on Systems*. 2025. Vol. 24. P. 91–105. DOI: https://doi.org/10.37394/23202.2025.24.11.

11. Mügge D. EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*. 2024. Vol. 31, № 8. P. 2200–2225. DOI: https://doi.org/10.1080/13501763.2024.2318475.

12. Swire P., Kennedy-Mayo D., Bagley D., Krasser S., Modak A., Bausewein C. Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*. 2024. Vol. 9, № 1. P. 20–51. DOI: https://doi.org/10.1080/23738871.2024.2384724.

13. Tropina T. «This is not a human rights convention!»: The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*. 2024. Vol. 9, № 2. P. 200–220. DOI: https://doi.org/10.1080/23738871.2024.2419517.

14. Bergaust J. C., Sellevåg S. R. Improved conceptualising of hybrid interference below the threshold of armed conflict. *European Security*. 2023. Vol. 33, № 2. P. 169–195. DOI: https://doi.org/10.1080/09662839.2023.2267478.

15. Thumfart J. Digital rights and the state of exception. internet shutdowns from the perspective of just securitization theory. *Journal of Global Security Studies*. 2024. Vol. 9, № 1. ogad024. DOI: https://doi.org/10.1093/jogss/ogad024.

16. Bachmann S.-D. D., Putter D., Duczynski G. Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*. 2023. Vol. 14, № 5. P. 858–869. DOI: https://doi.org/10.1111/1758-5899.13257.

17. Bidzilya Y., Solomin Y., Shvets V., Heletei A., Hetsko H. The media's

influence on shaping public opinion during martial law. *Journal of Intercultural Communication*. 2024. Vol. 24, № 4. P. 146–155. DOI: https://doi.org/10.36923/jicc.v24i4.979.

18. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.09.2025).

19. Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 № 47/2017. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 01.09.2025).

20. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 01.09.2025).

21. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 01.09.2025).

22. Про медіа : Закон України від 13.12.2022 № 2849-IX. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 01.09.2025).

23. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.11.2025).

24. National Cyber Security Index. *NCSI.* URL: https://ncsi.ega.ee/ncsi-index (дата звернення: 01.09.2025).

25. Internet Society Pulse. *Internet Society Pulse.* URL: https://pulse.internetsociety.org/about (дата звернення: 01.09.2025).

 ISSN: 3041-2110