HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА

СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 2021-2025 РОКІВ:

ОЦІНКА РЕАЛІЗАЦІЇ

Серпень - 2026

СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 2021-2025 РОКІВ: ОЦІНКА РЕАЛІЗАЦІЇ

Автори:

Павло Бурдяк, старший аналітик з цифрової безпеки Центру демократії та верховенства права

Олена Спесивцева, юристка з авторського права та медійного права напряму «Незалежні медіа» Центру демократії та верховенства права

Владислава Онищенко, молодша аналітикиня Центру демократії та верховенства права

Вікторія Митрофанова, асистентка проєктів в напрямку «Реформи державного управління» Центру демократії та верховенства права

Упорядники:

Тарас Шевченко, директор з розвитку Центру демократії та верховенства права

Олексій Третьяков-Гродзевич, менеджер проєктів, експерт у сфері реформи державного управління Центру демократії та верховенства права

Дослідження підготовлено Центром демократії та верховенства права за підтримки Фонду ім. Гайнріха Бьолля, Бюро Київ – Україна в межах проєкту «Адвокація та демократичний нагляд за розробкою та впровадженням Стратегії інформаційної безпеки України». Зміст публікації є відповідальністю Центру демократії та верховенства права та не є відображенням поглядів Фонду ім. Гайнріха Бьолля, Бюро Київ – Україна.

HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА

Зміст

ВСТУП

Захист інформаційного простору держави в умовах сучасних гібридних та воєнних загроз потребує чіткого стратегічного бачення, що визначає цілі, пріоритети й механізми реагування. Так, наприкінці 2021 року Указом Президента України від 28 грудня 2021 року № 685/2021 було введено в дію рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» та затверджено Стратегію інформаційної безпеки, розраховану на період до 2025 року. Перед завершенням підготовки і затвердженням наступного стратегічного документа і плану заходів необхідно підбити підсумки цього циклу: встановити, які цілі та завдання зберегли актуальність після початку повномасштабного вторгнення, які механізми довели свою практичну дієвість, що залишилося невиконаним або недостатньо результативним і які уроки мають бути враховані надалі.

Інформаційна безпека — невід'ємна складова національної безпеки. Інформаційні операції завжди супроводжували суспільно-політичні процеси, а надто під час війни. Проте внаслідок надшвидкого розвитку технологій і стирання віртуальних кордонів сучасне інформаційне середовище стало простором дешевого й ефективного впливу на суспільство, державні інституції та процеси ухвалення рішень, а інформаційні операції — одним із провідних засобів ведення війни. Повномасштабне вторгнення російської федерації не лише підсвітило значення інформаційного складника агресії, а й істотно змінило умови, в яких реалізовувалася Стратегія. Хоча цей документ і було затверджено у грудні 2021 року, проте План заходів з його реалізації ухвалили тільки у березні 2023 року. Отже, значна частина стратегічного циклу припала вже на період повномасштабної війни, що вимагало від державних органів адаптувати попередньо визначені завдання до нових загроз і потреб.

Оцінювати Стратегію слід із кількох позицій: власне досягнень та аналізу середовища на основі зовнішніх звітів — надто в часи тектонічних змін, таких як повномасштабна війна, стрімкий розвиток штучного інтелекту і трансформація способів створення й поширення інформації.

Саме тому оцінювання Стратегії не може обмежуватися формальним підрахунком виконаних заходів — необхідно з'ясувати, наскільки ефективно закладена у ній система дозволила державі реагувати на радикальну зміну безпекового середовища, чи забезпечила вона належну координацію між відповідальними суб'єктами та чи сприяли реалізовані заходи досягненню визначених цілей. Важливо також відокремити результати, безпосередньо пов'язані з виконанням Плану заходів, від ширших змін, спричинених війною, законодавчими реформами, діяльністю окремих органів або підтримкою міжнародних партнерів. Аналіз також охоплює відповідність між цілями Стратегії та заходами Плану, інституційну архітектуру й координацію, ресурсне забезпечення, взаємодію із громадянським суспільством і цифровими платформами, дотримання прав людини та систему моніторингу й оцінювання.

Проведений аналіз свідчить, що головний урок попереднього циклу — це необхідність посилити практичну орієнтацію стратегічного планування. Стратегія має бути не лише рамковим документом, що визначає загальні напрями державної політики, а й основою керованої системи її реалізації. Для цього потрібен чіткий зв'язок між

загрозами, цілями, завданнями й заходами, визначений розподіл сфер відповідальності, належне ресурсне забезпечення, дієві механізми координації, вимірювані показники результативності й можливість за потреби скоригувати державну політику відповідно до змін безпекового й технологічного середовищ.

Окремого опрацювання під час підготовки Стратегії на наступний період потребує питання її часової та предметної перспективи. Російська агресія, ймовірно, залишатиметься головним джерелом інформаційних загроз для України, тому її не можна розглядати лише як один із багатьох ризиків. Водночас кількарічний стратегічний документ має враховувати й ширші виклики, не обов'язково пов'язані з одним визначеним суб'єктом: трансформацію цифрового інформаційного середовища, розвиток генеративного штучного інтелекту, концентрацію впливу цифрових платформ та інші технологічні й суспільні ризики. Оптимальне співвідношення між фокусом на російській агресії та ширшою довгостроковою рамкою доцільно визначити за результатами окремої оцінки ризиків і консультацій із державними органами, сектором безпеки й оборони, представниками громадянського суспільства, медіа та експертною спільнотою.

Дослідження проводилося шляхом спілкування з експертами, аналізу документів і звітів, публічно наявної інформації та запитів, і виконувалося впродовж травня-серпня 2026 року.

МЕТОДОЛОГІЯ

Дослідження ґрунтується на якісному аналізі змісту Стратегії інформаційної безпеки України, Плану заходів із її реалізації та практики виконання цих документів у 2021–2025 роках. Основні джерела:

- текст Стратегії, затвердженої Указом Президента України від 28 грудня 2021 року №685/2021;
- План заходів, затверджений розпорядженням Кабінету Міністрів України від 30 березня 2023 року №272-р;
- офіційні звіти щодо виконання Плану заходів за 2023, 2024 і 2025 роки.

Додатково проаналізовано пов'язані нормативно-правові акти, стратегічні документи, офіційні повідомлення державних органів, а також документи у сфері інформаційної безпеки, стратегічних комунікацій та протидії інформаційним загрозам ЄС загалом і окремих європейських держав зокрема.

В оцінці реалізації ми розмежували: виконану роботу, наприклад, проведення заходів або підготовка матеріалів; безпосередні результати, зокрема створені продукти, ухвалені акти чи розбудована інфраструктура; ширші результати для відповідних аудиторій; довгостроковий вплив на інформаційну стійкість суспільства. Будь-який із розглянутих заходів не розглядався як результативний лише на підставі формального звіту про його проведення. Наскільки дозволяли джерела, ми зіставляли офіційні дані між роками та перевіряли їх на відповідність індикаторам Плану і заявленим стратегічним цілям.

Якісний аналіз нормативно-правових документів доповнений результатами двох експертних зустрічей, організованих Центром демократії та верховенства права (ЦЕДЕМ) спільно із Центром стратегічних комунікацій (ЦСК). У першій зустрічі взяло участь 20 представників експертної спільноти, у другій — 15. За їх результатами використали експертні оцінки як джерело професійної інтерпретації.

Дослідження має кілька обмежень. Офіційна звітність переважно ґрунтується на інформації самих виконавців і не передбачає системної незалежної верифікації. Структура звітів змінювалася, що ускладнило наскрізне порівняння результатів за роками. Крім того, значна частина індикаторів характеризує обсяг діяльності, а не її суспільний вплив. Тому там, де доступні дані не дозволяють встановити причиновий зв'язок між окремим заходом і досягненням стратегічної цілі, у дослідженні прямо зазначено цю невизначеність. Події після 2025 року враховані лише як подальший контекст і не включені до оцінки виконання Стратегії в межах установленого строку її реалізації.

1. КОНЦЕПТУАЛЬНА РАМКА СТРАТЕГІЇ

1.1. Місце Стратегії в системі стратегічних документів

Стратегія інформаційної безпеки — не автономний документ, адже він належить до системи планування у сферах національної безпеки і оборони. Так, Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року №392/2020, прямо визначила її одним із документів, що мають встановити способи та інструменти реалізації загальнодержавних безпекових пріоритетів. Рішення РНБО, введене в дію цим Указом, окремо доручило Кабінету Міністрів України та державним органам за відповідними сферами національної безпеки за пів року подати проєкт Стратегії інформаційної безпеки. Отже, необхідність її розробки випливала із визначеної архітектури стратегічних документів.

Стратегія національної безпеки надала майбутній секторальній Стратегії загальну ціннісну й понятійну рамку. В її основі — людина та захист її прав, державний суверенітет і територіальна цілісність, європейська та євроатлантична інтеграція, а також три засади державної політики: стримування, стійкість і взаємодія. Цей зв'язок простежується і безпосередньо у Стратегії інформаційної безпеки: стійкість і взаємодію визначено основними напрямами забезпечення інформаційної безпеки, а логіку стримування відтворено у інформаційних заходах оборони держави та у завданнях протидії інформаційним загрозам. Таким чином значна частина ключової термінології секторального документа походить із базової Стратегії національної безпеки, її слід розглядати у взаємозв'язку з нею.

Водночас функції двох документів відрізняються. Стратегія національної безпеки визначає загальну оцінку безпекового середовища, національні інтереси та міжсекторальні пріоритети, тоді як Стратегія інформаційної безпеки конкретизує їх для інформаційної сфери через перелік загроз, цілі й завдання, розподіл повноважень, механізми реалізації та очікувані результати. Тому якість секторальної Стратегії слід оцінювати, зокрема, за тим, наскільки послідовно вона переводить загальні положення Стратегії національної безпеки у практичну модель державної політики. Цей зв'язок має значення і для наступного стратегічного циклу: оновлення інформаційно-безпекової політики потребує узгодження з актуальною загальнодержавною оцінкою загроз, аби секторальні цілі, інституційна відповідальність, ресурси та індикатори не спиралися на рамку, сформовану для іншого безпекового середовища.

Безпосереднім попередником Стратегії 2021 року була Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року №47/2017, розроблена Міністерством інформаційної політики України і ухвалена РНБО 29 грудня 2016 року. Доктрина постала як відповідь на безпекову реальність після 2014 року, коли застосовувані російською федерацією технології гібридної війни перетворили інформаційну сферу на одну із ключових арен протиборства. Тоді наявні механізми державної інформаційної політики не забезпечували цілісної відповіді на пропаганду, інформаційно-психологічний вплив та окупацію частини інформаційного простору України.

Метою Доктрини було уточнення засад формування та реалізації державної інформаційної політики, передусім щодо протидії руйнівному інформаційному впливу російської федерації в умовах розв'язаної нею гібридної війни. Документ визначав національні інтереси в інформаційній сфері, загрози для їхньої реалізації, напрями й пріоритети державної політики та основні функції державних органів.

Між Доктриною 2017 року та Стратегією 2021 року існує певна змістовна спадкоємність: обидва документи поєднують безпекові завдання із гарантіями свободи слова, права на інформацію та приватність; приділяють увагу протидії російській пропаганді, розвитку й захисту інформаційної інфраструктури, підтримці української мови і культури, медіакультурі, зв'язкам із громадянами на тимчасово окупованих територіях та міжнародним комунікаціям. Стратегія також успадкувала сформований Доктриною понятійний апарат стратегічних, урядових і кризових комунікацій, а також стратегічного наративу. Таким чином Стратегія не започаткувала політику інформаційної безпеки з нуля, а систематизувала і розвинула підходи, напрацьовані в попередньому нормативному циклі.

Водночас Доктрина була переважно рамковим політико-безпековим документом і не формувала повного циклу стратегічного управління з визначеним строком реалізації, окремим планом заходів та системою вимірюваних показників. Стратегія 2021 року мала перевести ці засади у більш операційну форму: визначити стратегічні цілі та завдання, закріпити інституційні ролі, окреслити очікувані результати й передбачити план реалізації та щорічне звітування. Указ №685/2021 одночасно затвердив Стратегію та визнав такою, що втратила чинність, норму Указу №47/2017 про затвердження Доктрини. Тому співвідношення цих двох документів доцільно розглядати як послідовний перехід від доктринального визначення державної політики в умовах гібридної агресії до секторальної стратегії, вбудованої у систему планування, започатковану Стратегією національної безпеки 2020 року.

1.2. Українська специфіка: інформаційна агресія, окупація та реінтеграція

Поняття «інформаційна безпека» не має універсального й усталеного визначення в міжнародному чи європейському політико-правовому дискурсі. В Україні натомість забезпечення інформаційної безпеки України закріплено як один із основних напрямів державної інформаційної політики у статті 3 Закону України «Про інформацію», хоча сам Закон і не розкриває змісту цього поняття. В окремих актах українського законодавства інформаційна безпека визначається по-різному, переважно у технічному чи організаційно-технічному значенні. Відповідні визначення пов'язують її із забезпеченням конфіденційності, цілісності й доступності інформації, належного функціонування і стійкості електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем, а також із захистом від випадкових і навмисних загроз.

Значно ширше визначення інформаційної безпеки наведене безпосередньо у Стратегії інформаційної безпеки, що розглядає це поняття як складову національ-

ної безпеки та пов'язує її із захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших життєво важливих інтересів людини, суспільства і держави загалом. Такий підхід зумовлює широкий предмет Стратегії та її виразну безпекову спрямованість.

Перша змістовна специфіка Стратегії — широке розуміння інформаційної безпеки. Документ не зводить її виключно до протидії дезінформації, зловмисним інформаційним операціям та іншим формам шкідливого інформаційного впливу, а застосовує ширший підхід, за якого складові інформаційної безпеки — це забезпечення свободи слова, доступу до інформації, захист прав і безпеки журналістів, а також відкритість і прозорість діяльності органів державної влади. Така концепція має принципове значення для демократичної держави: реагування на інформаційні загрози має поєднуватися із захистом прав людини та збереженням умов для вільного суспільного обговорення. Отже, Стратегія виходить із необхідності балансу між безпекою інформаційного простору, з одного боку, та свободою вираження поглядів, доступом до інформації та демократичною підзвітністю держави — з іншого. Водночас практичне значення цього підходу залежить не лише від проголошення відповідних принципів, а й від їх імплементації.

Друга специфіка пов'язана з обставинами, за яких розробили та реалізували Стратегію. На відміну від стратегічних документів, що переважно мають перспективний характер і спрямовані на визначення потенційних ризиків, розвиток інституційних спроможностей та запобігання майбутнім загрозам, українська Стратегія інформаційної безпеки формувалася за принципово інших обставин. На момент її затвердження держава вже понад сім років протистояла не гіпотетичній, а безпосередній та системній інформаційній агресії російської федерації, що супроводжувала Помаранчеву революцію і Віктора Ющенка, а пізніше — Євромайдан і Революцію Гідності, а також окупацію Криму та окремих районів Донецької і Луганської областей. Стратегію ввели в дію 28 грудня 2021 року, а вже менш ніж за два місяці умови її реалізації радикально змінилися внаслідок початку повномасштабного вторгнення.

Саме ця обставина визначає другу особливість документа: він прямо називає російську федерацію основним джерелом загрози. Окремий блок Стратегії присвячений інформаційній політиці російської федерації, а серед національних загроз визначено інформаційний вплив держави-агресора на населення України. У документі йдеться про спеціальні інформаційні операції, спрямовані зокрема на підрив національної безпеки, ліквідацію української державності, знищення української ідентичності та дестабілізацію суспільно-політичної ситуації. Окремо названо спроби легітимізувати окупацію Криму, заперечити участь російської федерації у війні на Донбасі та поширити наратив про її нібито «громадянський» характер.

Третя особливість полягає в тому, що інформаційна агресія проти України має не лише комунікаційний або цифровий, а й територіальний та інфраструктурний виміри. Стратегія констатує захоплення на окупованих територіях об'єктів інформаційної інфраструктури, зокрема об'єктів Концерну радіомовлення, радіозв'язку та телебачення. Вона також фіксує встановлення державою-агресором контролю над місцевим інформаційним середовищем, як-от постачання на тимчасово окуповані території передавального обладнання та блокування українських інформаційних ресурсів, а також переслідування громадян за перегляд українського контенту. За таких

умов ідеться не лише про конкуренцію інтерпретацій у спільному інформаційному просторі, а й про власне фізичне і технологічне обмеження доступу до українського мовлення й інших джерел інформації.

Четверта взаємопов'язана змістовна особливість Стратегії — виокремлення інформаційної реінтеграції як самостійної стратегічної цілі. Документ передбачає відновлення права на інформацію громадян на тимчасово окупованих і прилеглих до них територіях, та підтримання їхнього зв'язку з Україною. Для цього визначено завдання щодо забезпечення стабільного функціонування національного телебачення і радіомовлення, розширення зони наземного ефірного мовлення із прилеглих територій, використання супутникових та інших каналів поширення сигналу, а також систематичного інформування про ситуацію на окупованих територіях і державну політику щодо їх реінтеграції.

Таким чином специфіку української Стратегії визначає поєднання чотирьох обставин: широке трактування інформаційної безпеки з урахуванням прав людини і демократичної підзвітності; пряме визначення російської федерації як джерела інформаційної агресії проти України; фізична окупація частини території та її інформаційної інфраструктури; необхідність підтримувати зв'язок із громадянами, у яких примусово обмежений доступ до українського інформаційного простору. Саме це поєднання відрізняє український підхід від стратегій, орієнтованих переважно на загальні технологічні ризики, кіберзагрози або стійкість до дезінформації. Водночас воно вимагає, щоб безпекова спрямованість державної політики інтегрувалася у захист свободи слова, права на інформацію та інші права людини.

1.3. Міжнародний досвід: ЄС, Естонія, Латвія, Молдова

Порівняльний аналіз міжнародного досвіду дає змогу встановити не лише те, які загрози визначають інші держави, а передусім те, як вони перетворюють стратегічні положення на систему координації, регулювання, моніторингу та практичних заходів. Водночас пряме перенесення іноземних моделей в український контекст було б недоцільним, оскільки жодна з розглянутих держав не реалізує політику інформаційної безпеки в умовах тривалої окупації частини території та повномасштабної збройної агресії. Тому відповідний досвід слід розглядати не як готову для впровадження модель, а як приклад окремих інституційних і управлінських рішень.

Для порівняння обрано Європейський Союз, держави-члени ЄС Естонію і Латвію, а також державу-кандидата на вступ до ЄС — Молдову. Рівень ЄС важливий з огляду на статус України як держави-кандидата і необхідність поступового наближення національного законодавства до нормативно-правових рамок Євросоюзу.

Естонія і Латвія цікаві нам як держави Балтії, що системно враховують російські інформаційні й гібридні операції у стратегічному плануванні. А Молдова — держава-кандидат на вступ до ЄС, яка прямо визначає росію та пов'язаних із нею суб'єктів як основне джерело довгострокових загроз, хоч і не перебуває у стані війни.

Рівень ЄС. Європейський Союз не має спеціальної стратегії інформаційної безпеки, що за своїм предметом повністю відповідала б українській. Натомість відповідна політика формується сукупністю взаємопов'язаних регуляторних і стратегічних інструментів, що охоплюють відповідальність цифрових платформ, свободу і плюралізм медіа, протидію іноземному інформаційному маніпулюванню та розвиток демократичної стійкості.

У 2025 році Європейська комісія представила Європейський щит демократії (European Democracy Shield — EDS) — загальну рамку, спрямовану на посилення демократичної стійкості, захист демократичних інститутів, цілісності інформаційного простору, а також протидію зовнішньому інформаційному втручанню. Передбачені документом заходи згруповані за трьома основними напрямами: захист цілісності інформаційного простору, зміцнення демократичних інститутів, вільних і чесних виборів та незалежних медіа, а також підвищення суспільної стійкості й участі громадян у демократичних процесах. Серед конкретних ініціатив визначені такі: підготовка протоколу реагування на інформаційні інциденти і кризи в межах DSA (Digital Services Act — Акт про цифрові послуги), оновлення інструментарію DSA для забезпечення чесних виборів, створення Європейської мережі фактчекерів (European Network of Fact-Checkers), подальша підтримка Європейської обсерваторії цифрових медіа (European Digital Media Observatory), розвиток медійної і цифрової грамотності і створення Європейського центру демократичної стійкості (European Centre for Democratic Resilience). Останній має сприяти обміну інформацією, оперативній співпраці та розвитку спроможностей між інституціями ЄС, державами-членами, а також державами-кандидатами (зокрема Україною) і потенційними кандидатами.

Центральне місце в регулюванні онлайн-платформ посідає DSA, що повністю застосовується із 17 лютого 2024 року. DSA не встановлює загальної заборони на дезінформацію і самостійно не визначає, який саме контент незаконний. Його основне значення — у запровадженні процедурних обов'язків для онлайн-посередників, а надто онлайн-платформ: прозорості правил модерації та звітування про неї, пояснення окремих рішень про обмеження контенту, внутрішнього оскарження, позасудового врегулювання спорів. Для дуже великих онлайн-платформ і пошукових систем передбачено додатковий обов'язок — виявляти, оцінювати та зменшувати системні ризики, пов'язані зокрема з негативним впливом на громадянський дискурс, виборчі процеси, громадську безпеку та основні права, а також із навмисним маніпулюванням їхніми сервісами.

Отже, DSA не пропонує державам модель безпосереднього контролю над правдивістю контенту, а переносить акцент із видалення окремих повідомлень на оцінювання того, як архітектура платформи, рекламні інструменти, алгоритмічні системи та скоординована поведінка можуть посилювати суспільні ризики. За результатами такого оцінювання найбільші онлайн-платформи та пошукові системи мають вживати обґрунтованих, пропорційних та ефективних заходів для мінімізації виявлених ризиків. Для України цей підхід важливий у двох аспектах: по-перше, наступна Стратегія має виразніше враховувати роль платформ як інфраструктури поширення інформації, а не лише як майданчиків для окремих випадків дезінформації та маніпуляцій. По-друге, взаємодія держави із платформами має ґрунтуватися на визначених процедурах, гарантіях прозорості й захисті прав користувачів, а не виключно на неформальних або ситуативних зверненнях.

Із DSA пов'язаний Кодекс практик щодо дезінформації (Code of Practice on Disinformation). Запроваджений у 2018 році як добровільний інструмент саморегулювання, Кодекс був істотно посилений у 2022 році. Його оновлена редакція містила 44 зобов'язання та 128 конкретних заходів, зокрема у сферах демонетизації дезінформації, прозорості політичної реклами, забезпечення цілісності сервісів, розширення можливостей користувачів, дослідників і фактчекерів. Із 2025 року він став релевантним орієнтиром для оцінювання виконання вимог DSA щодо мінімізації ризиків, пов'язаних із дезінформацією.

Інший важливий документ — Європейський акт про свободу медіа (European Media Freedom Act — EMFA). Він набув чинності у травні 2024 року, а більшість його положень застосовується із серпня 2025 року. Серед іншого, документ спрямований на захист редакційної незалежності, журналістських джерел і медіаплюралізму, підвищення прозорості власності і розподілу публічних коштів на державну рекламу.

Усі ці інструменти демонструють комплексний підхід: стійкість інформаційного простору забезпечує не лише протидія маніпулятивним кампаніям, а й прозорість платформ, незалежні медіа, доступ дослідників до даних, захист прав користувачів та інституційний нагляд. Українська Стратегія охоплює тією чи іншою мірою більшість цих вимірів — і незалежність медіа, і медіаграмотність, і інституційний нагляд, але проблемним аспектом, недостатньо покритим у Стратегії, лишається взаємодія із платформами: там, де ЄС перейшов до системних процедурних зобов'язань (оцінки ризиків, прозорості модерації, доступу дослідників до даних), українська практика значною мірою лишається на рівні ситуативних звернень і неформальної комунікації. DSA тут корисний як приклад перетворення відносин із платформами з ситуативних контактів на регульовану процедуру. Це може бути одним із орієнтирів під час розробки напряму взаємодії із платформами соцмереж.

Естонія. Естонія не має окремої стратегії інформаційної безпеки, подібної до української. Захист інформаційного середовища інтегрований у Концепцію національної безпеки 2026 року, в якій росію визначено найбільшою загрозою для Естонії та євроатлантичної безпеки.

Центральне поняття естонського підходу — «психологічна оборона», спрямована на зміцнення суспільної довіри, прагнення захищати державу та стійкості до ворожого впливу. Її нормативною основою визначено конституційні цінності, широке суспільне прийняття яких розглядається як передумова соціальної згуртованості (social cohesion) й відчуття безпеки (sense of security). Водночас захист інформаційного середовища і кіберпростору безпосередньо пов'язаний зі збереженням конституційного ладу, суверенітету й територіальної цілісності. Психологічна оборона реалізується через узгоджені позапартійні стратегічні комунікації із залученням суб'єктів від різних секторів суспільства.

Водночас Концепція передбачає своєчасне виявлення іноземних інформаційних маніпуляцій, зокрема дезінформації, і обмеження їхнього впливу. Таким чином естонська модель поєднує превентивний розвиток суспільної стійкості з оперативним реагуванням на конкретні інформаційні загрози.

Показовий елемент естонської моделі — закріплений у Концепції позапартійний (non-partisan) характер стратегічних комунікацій та залучення до них суб'єктів із різних секторів суспільства. Позапартійність передбачає інституційну сталість стратегічних комунікацій та їхню незалежність від зміни політичного керівництва.

Латвія. Інформаційна безпека закріплена на рівні Концепції національної безпеки Латвії 2023 року, що містить окремий розділ про запобігання загрозам інформаційному простору («Prevention of Threat Caused to the Information Space of Latvia»). Документ пов'язує такі загрози насамперед із російською пропагандою, дезінформацією та іншими інформаційними маніпуляціями, а серед пріоритетів визначає розвиток медіа- та інформаційної грамотності, підтримку сильних місцевих медіа, забезпечення безпеки журналістів і зміцнення єдиної державної стратегічної комунікації.

Секторальний документ — Національна концепція стратегічних комунікацій і безпеки інформаційного простору Латвії на 2023–2027 роки — за своєю суттю нагадує українську Стратегію. Вона поєднує розвиток державних стратегічних комунікацій, захист медіасередовища, медійну та інформаційну грамотність, співпрацю з громадянським суспільством, академічним і приватним секторами та міжнародними партнерами. Головним зовнішнім джерелом ризиків визначена росія, а її інформаційні кампанії проти Латвії розглядаються як довгострокова загроза, що триває з 1990-х років.

Центральну роль відіграє Державна канцелярія (State Chancellery), що планує національні стратегічні комунікаційні наративи та заходи на середньострокову та довгострокову перспективи. Це дає документу значно вищий рівень операційної деталізації: у ньому чітко прописані вимірювані цілі (наприклад, одна з них — досягнення показника 75% населення з розвинутими навичками медіаграмотності до 2027 року) та практичне рішення щодо аудиторії національних меншин: у короткостроковій перспективі — забезпечувати через наявні латвійські медіа альтернативний якісний новинний і розважальний контент без нарощування додаткового державного фінансування контенту мовами меншин; у середньо- та довгостроковій перспективі — сприяти інтеграції цієї частини суспільства до європейського медійного та інформаційного простору шляхом збільшення обсягу контенту латвійською мовою, сприяючи консолідації латвійського суспільства на основі державної мови.

Латвійський досвід показує доцільність встановлення вимірюваних цільових показників якісних змін у рівні стійкості суспільства. Водночас такі показники, зокрема бажаний рівень медіаграмотності, мають супроводжуватися сталою методикою вимірювання, інакше навіть чисельно визначена ціль не дає змоги надійно оцінити причиновий зв'язок між реалізацією стратегії та змінами у суспільстві.

Молдова. Стратегія національної безпеки Молдови, ухвалена у 2023 році, містить окремий напрям — Інформаційна безпека та стійкість (Information security and resilience). Вона визначає російську федерацію та її проксі найнебезпечнішим і найстійкішим джерелом загрози для молдовської державності, пов'язуючи його з інформаційними операціями, втручанням у вибори, підтримкою сепаратизму та іншими формами гібридного впливу.

Вимір інформаційної безпеки молдовської Стратегії доповнює секторальний документ — Концепція стратегічних комунікацій та протидії дезінформації, маніпулюванню інформацією та іноземному втручанню на 2024–2028 роки. Вона конкретизує розвиток державних стратегічних комунікацій, міжвідомчої системи раннього попередження, моніторингу та швидкого реагування, співпраці з медіа, громадянським суспільством і академічною спільнотою, а також заходів із медіаграмотності.

Концепція вибудовує рамкову основу для виконання місії Центру стратегічних комунікацій та протидії дезінформації, створеного Законом №242/2023 (із залученням українських консультантів). Водночас формування його операційної спроможності затягнулося: у 2024 році Європейська комісія констатувала необхідність посилити зусилля для забезпечення повної операційності ЦСК, а у 2025 році відзначила здійснення заходів із підвищення його операційної спроможності. Формальне створення спеціалізованого органу саме собою не забезпечує дієвої координації без належного ресурсного, кадрового й аналітичного забезпечення, визначених процедур міжвідомчої взаємодії та достатнього часу для інституційного становлення.

Загалом розглянутий міжнародний досвід свідчить, що ефективна політика інформаційної безпеки потребує не лише визначення загроз, а й вимірюваних цілей, належного ресурсного забезпечення та залучення медіа, громадянського суспільства і цифрових платформ. Для України ці елементи мають бути враховані у наступному циклі стратегічного планування з одночасним забезпеченням належних гарантій свободи слова.

Порівняння моделей інформаційної безпеки

	ЄС	Естонія	Латвія	Молдова
Основний документ	Європейський щит демократії (EDS), Акт про цифрові послуги (DSA), Європейський акт про свободу медіа (EMFA)	Концепція національної безпеки 2026	Концепція національної безпеки 2023 + Національна концепція стратегічних комунікацій 2023–2027	Стратегія національної безпеки 2023 + Концепція стратегічних комунікацій та протидії дезінформації, маніпулюванню інформацією та іноземному втручанню 2024–2028
Модель	Комплексна система регуляторних та стратегічних інструментів	Інтеграція інформаційної безпеки в національну безпеку	Окремий стратегічний напрям + секторальна концепція	Окремий напрям інформаційної безпеки + секторальний документ

	ЄС	Естонія	Латвія	Молдова
Ключовий фокус	Цілісність інформаційного простору та демократична стійкість	«Психологічна оборона» та суспільна стійкість	Стратегічні комунікації та медіаграмотність	Протидія дезінформації, іноземному втручанню та гібридним загрозам
Основні інструменти	DSA, Кодекс практик щодо дезінформації, EMFA, фактчекінг, EDMO, медіаграмотність	Стратегічні комунікації, раннє виявлення маніпуляцій, зміцнення суспільної довіри	Державні стратегічні комунікації, медіаграмотність, підтримка медіа, співпраця з громадянським суспільством	Раннє попередження, моніторинг, швидке реагування, стратегічні комунікації, співпраця з медіа та громадянським суспільством
Роль платформ / медіа	Системне регулювання платформ, прозорість модерації, оцінка системних ризиків	Стратегічні комунікації за участю різних секторів суспільства	Сильні місцеві медіа, безпека журналістів, альтернативний контент	Співпраця держави з медіа та громадянським суспільством
Сильна сторона моделі	Процедурність, системність і гарантії прав користувачів	Позапартійність та суспільна стійкість	Вимірювані цілі та висока операційна деталізація	Спеціалізований орган і система раннього реагування
Що важливо для України	Перехід від ситуативної взаємодії з платформами до чітких процедур	Інституційна сталість та позапартійність стратегічних комунікацій	Вимірювані показники результативності	Інституційна спроможність, ресурси та міжвідомча координація

2. ВІДПОВІДНІСТЬ СТРАТЕГІЇ МІНЛИВОМУ БЕЗПЕКОВОМУ СЕРЕДОВИЩУ

2.1. Зміна безпекового контексту у 2021–2025 роках

Стратегія інформаційної безпеки була затверджена 28 грудня 2021 року як секторальний документ, правовою основою якого, серед іншого, стала Стратегія національної безпеки України 2020 року. Менш ніж за два місяці після її затвердження російська федерація розпочала повномасштабну збройну агресію проти України. Тому оцінювання релевантності Стратегії потребує розмежування двох питань: наскільки документ відповідав безпековій ситуації на момент його розробки та наскільки закладена в ньому модель могла бути адаптована до принципово іншої реальності після 24 лютого 2022 року.

Вихідна оцінка загроз у Стратегії відображає безпековий контекст, сформований у 2014–2021 роках. Документ характеризує дії росії переважно через категорії гібридної війни, спеціальних інформаційних операцій, деструктивної пропаганди та інформаційного домінування на тимчасово окупованих територіях. Окупація Криму й окремих районів Донецької та Луганської областей розглядається як тривалий стан, навколо якого вибудовуються завдання інформаційної реінтеграції, забезпечення доступу до українського мовлення та протидії російським наративам. Згадка про пандемію COVID-19 як про один із чинників посилення ролі соціальних мереж також виразно відображає контекст підготовки документа.

Водночас ймовірність воєнної ескалації частково присутня у понятійних межах документа. Визначення поняття «інформаційних заходів оборони держави» охоплює дії в мирний час, в особливий період, під час воєнного або надзвичайного стану, зокрема заходи із протидії інформаційним загрозам з боку держави-агресора. Однак можливість воєнної ескалації розглядалася переважно як один із можливих правових і безпекових режимів, а не як сценарій, навколо якого вибудована окрема система цілей, координації та оцінювання результатів.

Саме в цьому полягає концептуальна відмінність між вихідною логікою Стратегії та практикою її реалізації у 2022–2025 роках. Адже документ визначає антикризові комунікації як заходи, спрямовані на запобігання кризовій ситуації. Ця конструкція передбачає можливість відокремити кризу від нормального режиму функціонування держави. Після 24 лютого 2022 року воєнний стан, бойові дії та постійний російський інформаційний вплив стали не окремою тимчасовою кризовою ситуацією, а тривалим середовищем діяльності практично всіх залучених органів.

Показово, що цю проблему визнає і підсумковий звіт за 2025 рік, де зазначено, що повномасштабне вторгнення перетворило інформаційний простір на повноцінний фронт бойових дій, це вимагає інших підходів до захисту й активної діяльності в інформаційній сфері. За оцінками авторів звіту, Стратегія була актуальною на момент її розробки, однак після 24 лютого 2022 року її положення значною мірою застаріли і стали недостатніми.

Отже, йдеться не про повну нерелевантність визначених у 2021 році цілей — протидія дезінформації, розвиток стратегічних комунікацій, медіаграмотності та інформаційної стійкості досі актуальні. Проте бракує вихідної концептуальної та операційної рамки для умов тривалої повномасштабної війни.

2.2. Урахування нових технологій

Зміст Стратегії відображає технологічне та безпекове середовище, що існувало на момент її ухвалення у грудні 2021 року. Документ розглядає поширення дезінформації, діяльність російських спецслужб, використання соцмереж та недостатню спроможність державних органів реагувати на інформаційні загрози. Водночас у характеристиці загроз, стратегічних цілях і напрямах реалізації не приділено окремої уваги генеративному штучному інтелекту, масовому створенню синтетичного контенту, дипфейкам, автоматизованому поширенню інформації та скоординованим мережам неавтентичної поведінки.

На момент розробки Стратегії окремі з цих технологій уже існували, однак не в нинішніх масштабах, вони не були доступними та не мали практичного значення для державної інформаційної політики. Тому їх відсутність не варто розглядати як первинний недолік документа — радше це свідчить про те, що визначена у 2021 році конфігурація загроз потребує актуалізації з урахуванням подальших технологічних змін інформаційного середовища.

До 2025 року необхідність актуалізації згаданих технологічних викликів стала очевидною. У підсумковій оцінці звіту Міністерства культури за 2025 рік зазначено, що ворожі інформаційні кампанії дедалі частіше використовують дипфейки, автоматизовану генерацію маніпулятивного контенту, мережі ботів та алгоритмічне просування дезінформації, що ускладнює оперативну перевірку інформації, збільшує навантаження на державні інституції та створює ризики масового поширення сфальсифікованого контенту. Таким чином технології, що не були окремо концептуалізовані у Стратегії 2021 року, наприкінці періоду її реалізації вже розглядали як один із визначальних чинників трансформації інформаційних загроз.

Звіт 2025 року показує і практичну значущість технологічно організованих мереж поширення інформації. За його даними, СБУ заблокувала вісім ботоферм, які поширювали матеріали, спрямовані на дискредитацію української влади та виправдовування російської агресії, а також мережу ботоферм у шести областях і ботоферму для створення бот-акаунтів через втручання в мережі мобільних операторів. CERT-UA, зі свого боку, протидіяла складним кібератакам угруповань APT28 і Sandworm проти органів державної влади, Сил оборони та об'єктів критичної інфраструктури. Ці приклади демонструють зближення інформаційних і кібернетичних загроз, яке лише частково охоплене загальними формулюваннями Стратегії.

Основна проблема полягає не в тому, що Стратегія 2021 року не передбачила подальший розвиток штучного інтелекту та інших технологій, а в тому, що за період її реалізації документ не був актуалізований відповідно до істотних і швидких змін ін-

формаційного середовища. Це визнає і підсумковий звіт: наявна модель інформаційної безпеки потребує суттєвого оновлення з огляду на застосування штучного інтелекту, дипфейків, автоматизованих мереж та алгоритмічного просування маніпулятивного контенту.

У новій Стратегії цей недолік слід усунути, переглянувши оцінки технологічних загроз і передбачивши механізм оперативного коригування цілей та заходів відповідно до істотних змін інформаційного середовища.

2.3. Взаємодія із цифровими платформами

У Стратегії правильно визначені соціальні мережі — як самостійні суб'єкти впливу в інформаційному просторі, що мають неабиякий вплив на суспільно-політичні процеси, реалізацію прав і свобод людини та захист приватності. Водночас це визнання залишилося переважно на рівні опису загроз, адже у Стратегії не визначено, який орган має координувати взаємодію держави із цифровими платформами, з яких саме питань, якими процедурами має регулюватися обмін інформацією та як оцінювати результативність такої взаємодії.

План заходів також не передбачав налагоджених механізмів взаємодії із цифровими платформами. Найближче за змістом завдання — запровадження механізму виявлення, фіксації, обмеження доступу та видалення з українського сегмента інтернету інформації, розміщення якої обмежене або заборонене законом. Однак такий механізм на ділі зводився до розробки алгоритмів реагування на гібридні загрози. Разом із цим варто визначити особливості співпраці із платформами, компетенції відповідальних органів, процедур направлення і розгляду запитів, вимог до звітності або гарантій від непропорційного обмеження законного контенту.

На практиці певна взаємодія все ж відбувалася. Так, у звіті за 2023 рік зазначено, що Центр протидії дезінформації (ЦПД) постійно моніторив відео на YouTube, і якщо контент певного каналу, за оцінкою Центру, загрожував національній безпеці та порушував українське законодавство, надсилав запит про його блокування безпосередньо відеохостингу.

Окремі механізми зв'язку із платформами є і в деяких інших українських державних профільних органів. Водночас звіт не розкриває правової природи таких механізмів, критеріїв направлення запитів, співвідношення поданих і задоволених звернень (втім, деяку загальну інформацію про звернення можна знайти на сайтах самих платформ), мотивів відмов або можливостей для захисту прав тих, чий контент було обмежено. Тому наведений приклад радше свідчить про ситуативну операційну практику, ніж про сформовану систему взаємодії.

Такий висновок узгоджується з підсумковою оцінкою за 2025 рік, де прямо зазначено, що взаємодія із цифровими платформами залишається недостатньо ефективною, тоді як доступ до алгоритмічних механізмів модерації та аналітичних даних платформ є обмеженим. Це один із ключових викликів реалізації Стратегії. Учасники експертної зустрічі, організованої ЦЕДЕМ і ЦСК, також звернули увагу на те, що доку-

мент не визначив, який саме орган мав би вести системний діалог із платформами. На думку експертів, подальший розвиток такої взаємодії залежить як від спроможності українських органів сформувати сталі механізми співпраці, так і від готовності самих платформ до діалогу.

Отже, прогалина полягає не у відсутності будь-яких контактів, а в тому, що окремі практики взаємодії не перетворили на сталі механізми співпраці з платформами, які спиралися б на спільно визначені цілі та процедури й мали чітке інституційне забезпечення.

У новій Стратегії доцільно визначити розвиток системної взаємодії із цифровими платформами як окремий напрям державної політики. Його метою має бути не лише оперативне реагування на окремі одиниці незаконного контенту, а й формування прозорої системи співпраці, що охоплюватиме забезпечення належних процедур модерації, протидію координованим інформаційним операціям, захист прав користувачів та поступове наближення України до регуляторної моделі DSA.

Чому стратегія інформаційної безпеки 2021 року стала недостатньою після 24 лютого 2022 року

ВИХІДНА МОДЕЛЬ

28 грудня 2021 року

2021

Стратегія інформаційної безпеки затверджена.

- Гібридна війна
- Дезінформація та пропаганда
- Російські наративи
- Окуповані території
- Стратегічні комунікації
- Соцмережі — важливий канал впливу

ПЕРЕЛОМ

24 лютого 2022 року

2022

Повномасштабне вторгнення росії в Україну.

- Воєнний стан
- Бойові дії стають постійним середовищем функціонування держави
- Пріоритет — виживання та оборона

НОВА РЕАЛЬНІСТЬ

2023

Інформаційний простір перетворюється на повноцінний фронт війни.

- Постійна інформаційна війна
- «Антикризова» модель уже не відповідає тривалому характеру загроз
- Зростання впливу соціальних мереж та месенджерів
- Посилення кібератак

2024

ТЕХНОЛОГІЧНИЙ СТРИБОК

Нові технології кардинально змінюють характер загроз.

- Генеративний ШІ та дипфейки
- Ботоферми та автоматизоване поширення контенту
- Алгоритмічне просування дезінформації
- Перетин інформаційних та кібернетичних загроз
- Зростання швидкості та масштабів впливу

ТОЧКА ПЕРЕОЦІНКИ

2025

Підсумкова оцінка ефективності Стратегії 2021 року.

- Стратегія була актуальною у 2021 році
- Після 24.02.2022 її положення значною мірою стали недостатніми
- Потрібне концептуальне та операційне оновлення

3. МЕХАНІЗМИ РЕАЛІЗАЦІЇ СТРАТЕГІЇ

3.1. Інституційна архітектура та координація

3.1.1. Розподіл повноважень

Стратегія інформаційної безпеки передбачила багаторівневу й переважно децентралізовану модель реалізації державної політики. На загальнодержавному рівні координацію діяльності органів виконавчої влади в інформаційній сфері мала здійснювати Рада національної безпеки і оборони України, зокрема з використанням спроможностей ЦПД.

Указ Президента України від 7 травня 2021 року №187/2021, яким затверджено Положення про ЦПД, окремо зобов'язав Кабінет Міністрів забезпечити взаємодію центральних органів виконавчої влади із Центром, зокрема через участь у нарадах, розробці нормативних актів та обміні необхідною інформацією. Завдання ЦПД полягало в протидії поточним і прогнозованим загрозам національній безпеці в інформаційній сфері, виявленні дезінформації, протидії пропаганді та деструктивним інформаційним впливам.

На Кабінет Міністрів України Стратегія поклала формування і реалізацію державної інформаційної політики, забезпечення інформаційного суверенітету, фінансування відповідних програм, а також спрямування і координацію роботи міністерств та інших органів виконавчої влади. Кабінет Міністрів також мав затвердити план заходів для органів виконавчої влади для реалізації Стратегії.

Галузеві повноваження були розподілені між широким колом суб'єктів. Центральний орган виконавчої влади, відповідальний за формування і реалізацію державної політики в інформаційній сфері, мав здійснювати нормативно-правове регулювання, визначати перспективи та пріоритетні напрями розвитку інформаційної безпеки і спільно з Міністерством закордонних справ сприяти популяризації України та формуванню її позитивного іміджу за кордоном. Міністерство оборони та сили оборони відповідали, серед іншого, за моніторинг загроз у воєнній сфері, проведення інформаційних заходів оборони, координацію залучення до них суб'єктів безпекового сектора і розвиток системи стратегічних комунікацій. Окремі функції щодо виявлення та протидії інформаційним загрозам були закріплені за Службою безпеки України, розвідувальними органами та Національною радою України з питань телебачення і радіомовлення. Реалізація Стратегії мала також відбуватися у взаємодії з органами місцевого самоврядування та інститутами громадянського суспільства.

Такий розподіл відповідав комплексному характеру інформаційної безпеки, що охоплює державні комунікації, протидію ворожим інформаційним операціям, медійну політику, міжнародне інформування, діяльність сектора безпеки і оборони та розвиток суспільної стійкості. Тому множинність суб'єктів не слід оцінювати як недолік. Централізація всіх функцій в одному органі навряд чи була б реалістичною або бажаною. Проблема полягала в іншому: Стратегія визначала галузеві функції

окремих органів, однак процедури їхньої постійної горизонтальної взаємодії не були чітко прописаними. Так, Стратегія покладала координацію діяльності органів виконавчої влади у сфері інформаційної безпеки на РНБО, тоді як Кабінет Міністрів України координував роботи міністерств та інших органів виконавчої влади. Водночас документ лише в загальних рисах визначав співвідношення між цими координаційними функціями та не конкретизував постійні процедури горизонтальної взаємодії між виконавцями, зокрема порядок обміну аналітичною інформацією, узгодження міжвідомчих рішень і координації кризового реагування.

Особливе місце в інституційній архітектурі посідало профільне міністерство. Після затвердження Плану заходів саме Міністерство культури та інформаційної політики мало відстежувати його виконання за допомогою електронної системи моніторингу і контролю та щороку до 15 квітня подавати узагальнений звіт Апарату РНБО і Кабінету Міністрів. Інші міністерства й центральні органи виконавчої влади мали щороку до 1 березня подавати міністерству інформацію, яку включали у цей звіт. Таким чином міністерство виконувало функцію адміністративного координатора виконання Плану.

Окремо варто згадати, що інституційна сталість цієї системи була додатково ускладнена реорганізаціями профільного міністерства. У вересні 2024 року Міністерство культури та інформаційної політики перейменували на Міністерство культури та стратегічних комунікацій. А наприкінці 2025 року уряд змінив назву на «Міністерство культури України» та перерозподілив частину повноважень між Держкомтелерадіо і Міністерством. Водночас за останнім було збережено формування державної політики у сфері інформаційної безпеки, але низку положень, пов'язаних із державним іномовленням, популяризацією України та стратегічними комунікаціями, із положення про нього вилучили.

Ці зміни відбулися на завершальному етапі реалізації Стратегії, тому їхній довгостроковий вплив не можна оцінити лише за звітами 2023–2025 років. Проте вони засвідчують інституційну несталість самої моделі: орган, який координував виконання Плану та збирав звітність, протягом періоду реалізації Стратегії пройшов через зміну назви, напрямків роботи та розподілу повноважень з іншими органами.

3.1.2. Координаційні механізми, передбачені Планом заходів

План заходів конкретизував окремі елементи міжвідомчої взаємодії. Зокрема, у межах завдання № 40 стратегічної цілі № 6 він передбачав співпрацю між центральними органами виконавчої влади для підвищення якості комунікації із суспільством відповідно до принципу «єдиного голосу» — функціонування єдиної інформаційної платформи стратегічної комунікації, підготовку методичних матеріалів, розробку механізму міжвідомчої координації у сфері протидії інформаційним загрозам, а також взаємодію між суб'єктами стратегічних комунікацій сил оборони.

Водночас спосіб організації цих заходів мав деякі недоліки. По-перше, центральний захід, спрямований на розроблення механізму міжвідомчої координації органів державної влади з протидії загрозам та викликам національній безпеці в інформаційній сфері (стратегічна ціль № 6, завдання № 40, захід № 4), був сформу-

льований абстрактно. Індикатором його виконання визначено сам факт розробки такого механізму, без уточнення його правової форми, складу учасників, порядку та періодичності роботи або якісних критеріїв оцінювання ефективності.

По-друге, індикатором налагодження співпраці відповідно до принципу «єдиного голосу» було визначено лише проведення заходів. Це дозволяло формально звітувати про виконання на підставі нарад або консультацій, однак не давало змоги встановити, чи стала координація регулярною, чи скоротився час реагування на кризові ситуації та чи були усунуті суперечності між повідомленнями різних органів тощо.

По-третє, План поєднав кілька різних рівнів координації: загальнодержавну взаємодію, координацію в секторі безпеки і оборони, відносини держави із громадськістю та медіа, а також міжнародні комунікації. Однак він не пояснював співвідношення між цими рівнями, і це створювало можливість розвитку паралельних механізмів, кожен із яких міг бути ефективним у своєму секторі, але не обов'язково був інтегрований у спільний цикл аналізу, планування, реалізації та оцінювання.

Звіти щодо виконання Плану заходів із реалізації Стратегії інформаційної безпеки за період до 2025 року фіксують низку практичних механізмів координації. Міністерство культури України проводило координаційні зустрічі з виконавцями Плану. Міністерство оборони забезпечувало роботу міжвідомчої групи із синхронізації повідомлень органів сектора безпеки і оборони. У системі МВС діяла Координаційна група зі стратегічних комунікацій, що проводила регулярні наради та готувала комунікаційні рамки й узгоджені повідомлення. Міністерство закордонних справ координувало публічну дипломатію та міжнародні інформаційні кампанії, зокрема у взаємодії із закордонними дипломатичними установами й Українським інститутом.

У звіті за 2025 рік зазначено, що Міноборони використовувало міжвідомчу координаційну групу та щотижневі синхронізаційні наради комунікаційних підрозділів. МВС провело два очні засідання і понад 40 щотижневих онлайн-нарад своєї Координаційної групи, а МЗС проводило стратегічні сесії з Українським інститутом, закордонними дипломатичними установами, профільним міністерством, МОН та Українським інститутом національної пам'яті. Все це свідчить про те, що у процесі реалізації Стратегії були сформовані або посилені сталіші механізми, принаймні в окремих секторах.

Разом із тим офіційні звіти самі визнають обмеження наявної моделі координації. Так, у звіті за 2024 рік зазначено, що єдина централізована модель координації перебувала на етапі становлення, а взаємодія між суб'єктами мала переважно секторальний або проєктний характер. У підсумковій частині документа серед проблем названо недостатню горизонтальну узгодженість і відсутність сталого координаційного центру. Звіт за 2025 рік також констатує, що у сфері кризових комунікацій та оперативного реагування на інформаційні загрози координація лишалася недостатньо інтегрованою. Відсутність єдиної державної системи кризових комунікацій і швидкого міжвідомчого обміну аналітичними даними, за оцінкою самого міністерства, ускладнювала комплексне реагування на масштабні й транснаціональні інформаційні операції.

Таким чином офіційні матеріали демонструють одночасно два процеси: розвиток практичної взаємодії та незавершеність її системної інституціоналізації. Кількість нарад, робочих груп або підготовлених комунікаційних рамок підтверджує певну діяльність, але не достатня для висновку про існування цілісної загальнодержавної системи. Для цього необхідні були б дані про сталість відповідних механізмів, швидкість міжвідомчого обміну інформацією, обов'язковість узгоджених рішень, охоплення всіх основних суб'єктів і вплив координації на результати державної політики. Таких даних у звітах наведено недостатньо.

Крім того, на основі експертних зустрічей, організованих ЦЕДЕМ спільно із Центром стратегічних комунікацій, можна виокремити кілька додаткових проблем фактичного функціонування системи. Учасники звернули увагу на те, що міжвідомча координація залишалася дуже персоналізованою та залежала від конкретних посадовців. Тобто окремі формати взаємодії, на думку експертів, працювали завдяки професійним контактам і особистій ініціативі, але не були закріплені як сталі процедури.

На цих зустрічах експерти також звертали увагу на відсутність єдиного підходу до оцінювання ефективності стратегічних комунікацій, а також на те, що не було чітко визначено орган, відповідальний за ведення системного діалогу з цифровими платформами.

Експерти зійшлися на тому, що окремі елементи системи стратегічних комунікацій хоч і створені, проте вони не були повністю інтегровані в єдину архітектуру. Як основні проблеми визначені такі: розпорошення відповідальності, інституційні реорганізації, нерівномірність кадрових спроможностей і проєктний характер частини взаємодії. Водночас учасники визнали результативність окремих механізмів, особливо у секторі безпеки й оборони, міжнародних комунікаціях, професійній підготовці та співпраці із громадянським суспільством.

Отже, стратегія сформувала широкий перелік суб'єктів інформаційної безпеки та загалом обґрунтовано розподілила між ними галузеві функції. У процесі її реалізації були створені чи розвинені працездатні механізми взаємодії, насамперед у секторі безпеки і оборони, системі МВС, міжнародних комунікаціях, інформаційних активностях та підготовці держслужбовців.

Водночас Стратегія і План заходів не завершили формування єдиного механізму горизонтальної координації. Ролі РНБО, Кабінету Міністрів, профільного міністерства, Центру протидії дезінформації, Центру стратегічних комунікацій та галузевих органів були визначені на різних рівнях узагальнення, але порядок їхньої взаємодії залишився недостатньо конкретизованим. План передбачив розробку міжвідомчого механізму, однак не встановив його обов'язкових характеристик і не запропонував критеріїв для оцінки його реального функціонування. Адміністративний моніторинг виконання Плану також не був підкріплений чіткими повноваженнями координатора щодо перевірки результатів або коригування діяльності виконавців.

У 2021–2025 роках Україна розвинула широку мережу інституцій і секторальних механізмів стратегічних комунікацій, однак не вибудувала з них цілісну систему.

Сильними сторонами моделі були професіоналізація окремих структур, розвиток координації у секторі безпеки й оборони, активізація міжнародних комунікацій та спроможність швидко формувати кризові формати взаємодії. Її основними обмеженнями залишалися фрагментарність і несталість інституційного дизайну, недостатня формалізація горизонтальної координації та відсутність єдиної системи оцінювання результатів. Це свідчить не стільки про відсутність інституційної архітектури, скільки про незавершеність її формування.

3.2. Взаємодія з організаціями громадянського суспільства

Стратегія інформаційної безпеки прямо визнає інститути громадянського суспільства учасниками формування та реалізації державної політики в інформаційній сфері. Насамперед у межах стратегічної цілі № 1 «Протидія дезінформації та інформаційним операціям» одним із завдань визначено забезпечення ефективної взаємодії державних органів, органів місцевого самоврядування та інститутів громадянського суспільства під час формування і реалізації державної політики в інформаційній сфері. Отже, документ передбачає залучення громадянського суспільства не лише як виконавця окремих інформаційних або освітніх проєктів, а і як учасника процесу формування відповідної політики.

Положення про взаємодію із громадськістю містяться також у стратегічній цілі № 6 «Створення ефективної системи стратегічних комунікацій». Основною метою цієї системи визначено забезпечення ефективної інформаційної взаємодії та діалогу між органами державної влади, органами місцевого самоврядування і суспільством із питань кризових ситуацій. Окремим завданням передбачено налагодження ефективної співпраці між представниками держави та громадськістю через системний діалог державних органів із медіа, журналістами та представниками нових медіа у кризових ситуаціях та у післякризовий період.

Крім того, стратегічна ціль № 7 «Розвиток інформаційного суспільства та підвищення рівня культури діалогу» передбачає публічне обговорення актуальних проблем інформаційного суспільства та його розвитку. Це положення створювало додаткову основу для проведення консультацій із громадськістю, хоча безпосередньої участі ОГС у моніторингу та перегляді Стратегії не регламентувало.

Згадані положення щодо ОГС доповнені у розділі VII «Механізми реалізації визначеної мети та завдань», де встановлено, що органи державної влади у взаємодії з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства забезпечують реалізацію Стратегії за затвердженим Кабінетом Міністрів планом заходів. Таким чином взаємодія з ОГС закріплена одночасно як окремі завдання стратегічних цілей № 1, 6 і 7 та як загальний механізм реалізації всього документа.

Певний парадокс, однак, полягає в тому, що організації громадянського суспільства, яким Стратегія відводила роль у формуванні державної політики в інформаційній сфері, за свідченнями учасників експертних зустрічей, не були достатньо

залучені до розробки власне тексту Стратегії. Підготовка документа спиралася на роботу групи представників державних органів, тоді як позиції громадянського суспільства у питанні інформаційної безпеки, за свідченнями деяких учасників експертних зустрічей ЦЕДЕМ і Центру стратегічних комунікацій, не були враховані.

Звіти про виконання Плану заходів засвідчують, що взаємодія державних органів із ОГС була наповнена співпрацею. Так, у 2023 році Центр стратегічних комунікацій повідомив про створення спільних інформаційних продуктів із VoxCheck та іншими медійними партнерами, зокрема подкасту «ПОГОВОРИМО». Міністерство культури України спільно із ЦЕДЕМ проводили тренінги для розпорядників публічної інформації. Міністерство освіти і науки (МОН) разом із IREX та у співпраці з Академією української преси працювали над реалізацією проєкту «Вивчай та розрізняй: інфомедійна грамотність в освіті».

У 2024 році найпослідовнішою була співпраця у сфері медіаграмотності. Національний проєкт «Фільтр» проводив щоквартальні координаційні зустрічі зі стейкхолдерами, а у співпраці з МОН та IREX був організований Національний тест із медіаграмотності. Проєкт «Вивчай та розрізняй», за даними звіту, охопив 2416 закладів освіти та 5309 учителів. Взаємодія з громадськістю відбувалася також у консультаційному форматі: МКСК повідомило про проведення 14 консультацій щодо проєктів нормативно-правових актів. Також у МКСК, в тому числі під час кризи, пов'язаної з реорганізацією Центру стратегічних комунікацій, була створена Експертна група з формування системи державних стратегічних комунікацій.

У 2025 році співпраця у сфері медіаграмотності охоплювала освітні, координаційні та аналітичні формати. Так, 21 травня відбулася зустріч понад 20 представників державних структур, громадського сектора та міжнародних організацій, під час якої обговорювали фінансову стійкість проєктів і нові формати взаємодії. У співпраці з ЦЕДЕМ та International Media Support було створено Академію відповідального використання ШІ «ПРОМПТО». На запит Мінкульту підготовлено дослідження ринку медіаграмотності України (ГО «Інститут свідомого громадянства» та ініціатива «Як не стати овочем», реалізовано Zinc Network за підтримки МЗС Великої Британії).

Громадські організації водночас реалізовували власні ініціативи у сферах, охоплених Стратегією. У ході експертного обговорення фахівці зазначали, що протягом періоду дії та реалізації Стратегії в Україні збереглася й посилилася екосистема громадських організацій, фактчекерів, аналітичних центрів і медіа, залучених до протидії дезінформації. Як приклад наводили Індекс медіаграмотності українців «Детектор медіа», що давав змогу простежувати загальну динаміку медіаграмотності населення. Учасники експертної дискусії також звертали увагу на те, що громадський сектор продовжував діяльність навіть за умов скорочення донорського фінансування та недостатньої державної підтримки.

Наведені приклади дають підстави позитивно оцінювати внесок громадянського суспільства у виконання Стратегії. Співпраця з державою охоплювала фактчекінг, медіаграмотність, навчання розпорядників публічної інформації, підготовку аналітичних досліджень, створення інформаційних продуктів і проведення громадських консультацій. У деяких напрямах, передусім у сфері медіаграмотності, така

співпраця стала регулярною. ОГС не лише долучалися до державних заходів, а й забезпечували власну експертизу, методики та інструменти оцінювання, частково доповнюючи діяльність державних інституцій.

Водночас йдеться переважно про секторальний і проєктний характер цієї взаємодії. По-перше, регулярність співпраці простежувалася лише в окремих напрямах і дуже залежала від ініціатив конкретних державних органів, проєктів або партнерських організацій. По-друге, участь ОГС не була оформлена як постійний і представницький механізм, що охоплював би весь стратегічний цикл: формування політики, виконання заходів, моніторинг, оцінювання результатів і перегляд Плану. По-третє, не були визначені прозорі принципи залучення організацій, порядок подання ними пропозицій та механізм зворотного зв'язку щодо їх урахування. По-четверте, звітність переважно фіксувала кількість зустрічей, тренінгів, консультацій, досліджень та інформаційних продуктів, але не давала змоги встановити, як саме співпраця з ОГС вплинула на державні рішення, результативність політики та цільової аудиторії ініціатив із медіаграмотності. Врешті-решт, залежність значної частини спільних ініціатив від міжнародної донорської підтримки створювала ризики для їхньої фінансової та інституційної сталості.

Отже, проблема полягала не лише в недостатній інституціоналізації взаємодії під час виконання Стратегії, а й у неналежному залученні ОГС на етапі підготовки самої Стратегії та Плану заходів. Це створило розрив між задекларованою роллю громадянського суспільства у формуванні державної інформаційної політики та практикою розробки документів, що визначали її зміст і механізми реалізації. Під час підготовки наступної Стратегії цей недолік слід усунути, залучивши на ранньому етапі представників ОГС до системного визначення проблем, формулювання цілей і завдань, розробки заходів та показників їх виконання. Надалі такий формат співпраці має охоплювати весь стратегічний цикл, зокрема моніторинг, оцінювання та періодичний перегляд заходів. Для цього варто встановити прозору процедуру відбору учасників, порядок подання пропозицій і обґрунтований зворотний зв'язок щодо їх урахування, а також передбачити сталі моделі ресурсного забезпечення спільних ініціатив. Це дозволило б закріпити роль громадянського суспільства не лише як виконавця чи партнера окремих проєктів, а як повноцінного учасника формування, реалізації та оцінювання державної політики у сфері інформаційної безпеки.

3.3. Фінансове забезпечення реалізації Стратегії

Стратегія інформаційної безпеки не містить окремого розділу чи додатка, присвяченого її фінансовому забезпеченню. Водночас у розділі «Механізми реалізації визначеної мети та завдань» на Кабінет Міністрів покладено, серед іншого, фінансування програм, пов'язаних з інформаційною безпекою, а серед напрямів реалізації стратегічної цілі № 7 окремо згадано забезпечення належного фінансування суспільного мовника. Однак Стратегія не визначає орієнтовної вартості її реалізації, джерел фінансування окремих напрямів, порядку розподілу ресурсів між виконавцями або механізму консолідованого фінансового моніторингу.

Ця прогалина не усунута і у Плані заходів, затвердженому Кабінетом Міністрів у березні 2023 року. План визначає заходи, строки їх виконання, відповідальних суб'єктів та індикатори, але не містить окремої графи щодо необхідного обсягу або джерела фінансування. Відповідно ресурсне забезпечення заходів фактично фінансувалося із бюджетних програм та через кошториси окремих органів-виконавців, а також із залученням міжнародної допомоги. Такий підхід дозволяє розподілити фінансове навантаження між установами, але не дає змоги на рівні самого Плану встановити, чи кожен захід був забезпечений достатніми ресурсами та скільки коштів сукупно спрямовано на реалізацію Стратегії.

Практичні наслідки цієї моделі простежуються, наприклад, у звіті за 2025 рік. У межах стратегічної цілі № 2 конкурсні відбори кінопроєктів для підтримки українського кіновиробництва не проводилися через бюджетні обмеження. У підсумковій частині звіту відсутність фінансування кіногалузі охарактеризована як «критично незакрита прогалина», що ставить під загрозу наступний виробничий цикл. Отже, принаймні щодо окремих завдань нестача фінансування безпосередньо вплинула не лише на масштаб, а й на саму можливість їх виконання.

Інший аспект — значна роль міжнародної підтримки у виконанні окремих заходів із медіаграмотності. У 2025 році в межах національного проєкту «Фільтр» реалізовано інтерактивну квест-кімнату «Петля часу» за підтримки ПРООН та уряду Японії, а конкурс учнівських відеосюжетів «Репортер 2025» — за підтримки Ради Європи. Залучення донорських ресурсів дає змогу розширювати масштаб ініціатив, використовувати міжнародну експертизу та реалізовувати проєкти, для яких державного фінансування могло би бути недостатньо. Водночас учасники експертних зустрічей, проведених у межах цього дослідження, звертали увагу на необхідність забезпечення фінансової стійкості проєктів у сфері медіаграмотності. Тобто міжнародна підтримка — це важливий додатковий ресурс для реалізації відповідного напряму, проте надмірна залежність від неї за відсутності передбачуваного державного фінансування ускладнює довгострокове планування, безперервність і масштабування успішних ініціатив.

Децентралізований характер фінансування особливо помітний у межах стратегічної цілі № 1, до виконання якої залучено чимало органів державної влади та установ. Кожен із них фінансує відповідну діяльність через власні бюджетні програми та кошторисні призначення. Перевага такої моделі — включення інформаційної безпеки у поточну діяльність різних інституцій. Водночас відсутність єдиного бюджетного координатора та консолідованої фінансової звітності ускладнює оцінювання необхідного рівня ресурсів, виявлення недофінансованих завдань і визначення сукупної вартості реалізації Стратегії.

Отже, проблема полягає у відсутності бюджетного планування на рівні Стратегії і Плану заходів. Звіти про виконання Стратегії підтверджують практичне значення цієї прогалини: нестача ресурсів уже призвела до невиконання окремих заходів, тоді як частина ініціатив реалізовувалася за підтримки міжнародних партнерів. У наступній редакції Стратегії та плану заходів доцільно передбачити фінансову рамку, що визначатиме джерела фінансування, відповідальність за його координацію та порядок щорічного звітування про заплановані й фактичні витрати.

3.4. Система моніторингу та оцінювання виконання Стратегії

План заходів передбачав формальну систему моніторингу його виконання. На Міністерство культури України було покладене оцінювання із використанням електронної системи моніторингу і контролю на Єдиному вебпорталі електронного урядування, що так і не був створений, а також щорічне подання звіту до 15 квітня Апарату РНБО та Кабінету Міністрів про виконання Плану — ці звіти публічно доступні. Для координації цієї роботи Міністерство проводило зустрічі із представниками органів, відповідальних за реалізацію передбачених Планом заходів. Отже, на інституційному рівні координуючий орган та регулярний цикл звітування були визначені.

Практика звітування поступово змінювалася. Звіт за 2023 рік містив деталізовану інформацію від виконавців щодо окремих заходів Плану. У звітах за 2024 і 2025 роки матеріал узагальнили за стратегічними цілями. Структура звітів передбачала опис ключових заходів та вимірюваних показників, виявлених проблем і рекомендацій щодо коригування завдань. Такий перехід до аналітичного формату — цілком позитивний, оскільки він дозволив вийти за межі механічного переліку дій і сформувати загальне уявлення про реалізацію кожної стратегічної цілі. Водночас зміна структури звітів і неповне відтворення у пізніших звітах інформації про заходи, виконані раніше, ускладнювали наскрізне відстеження прогресу протягом усього періоду реалізації Стратегії.

Основне обмеження системи полягало в тому, що вона була орієнтована переважно на моніторинг діяльності, а не на оцінювання її результатів та імпакту (впливу). Значна частина індикаторів Плану фіксувала проведення заходів, підготовку матеріалів, створення продуктів, ухвалення документів або кількість поінформованих осіб. Такі показники дозволяли встановити, чи виконавець реалізував заплановану дію, однак не давали змогу з'ясувати, чи сприяла вона досягненню стратегічної цілі. Наприклад, кількість проведених тренінгів сама собою не показує, чи покращилися знання чи поведінка учасників, а кількість інформаційних матеріалів — чи вплинули вони на цільову аудиторію та посилили її стійкість до інформаційних впливів. У звітах щодо виконання Плану заходів є низка кількісних показників, але недостатньо розвинена єдина система оцінювання власне ефективності всіх цих заходів.

Втім, окремі звіти намагалися оцінювати не лише активність, а й результативність. Зокрема, звіт за 2024 рік наводив відсоткові показники реалізації заходів та ефективності реагування, порівнював окремі дані з попереднім звітним роком і характеризував зміни суспільних показників. Проте методика розрахунку частини таких показників, їхні базові та цільові значення, а також зв'язок із конкретними індикаторами Плану не завжди були прозорими і зрозумілими. Крім того, у звітах переважно узагальнювали інформацію, надану відповідальними органами. Водночас ані Стратегія, ані План заходів не передбачали окремої процедури незалежної верифікації наданих даних або періодичного зовнішнього оцінювання результативності реалізації Стратегії.

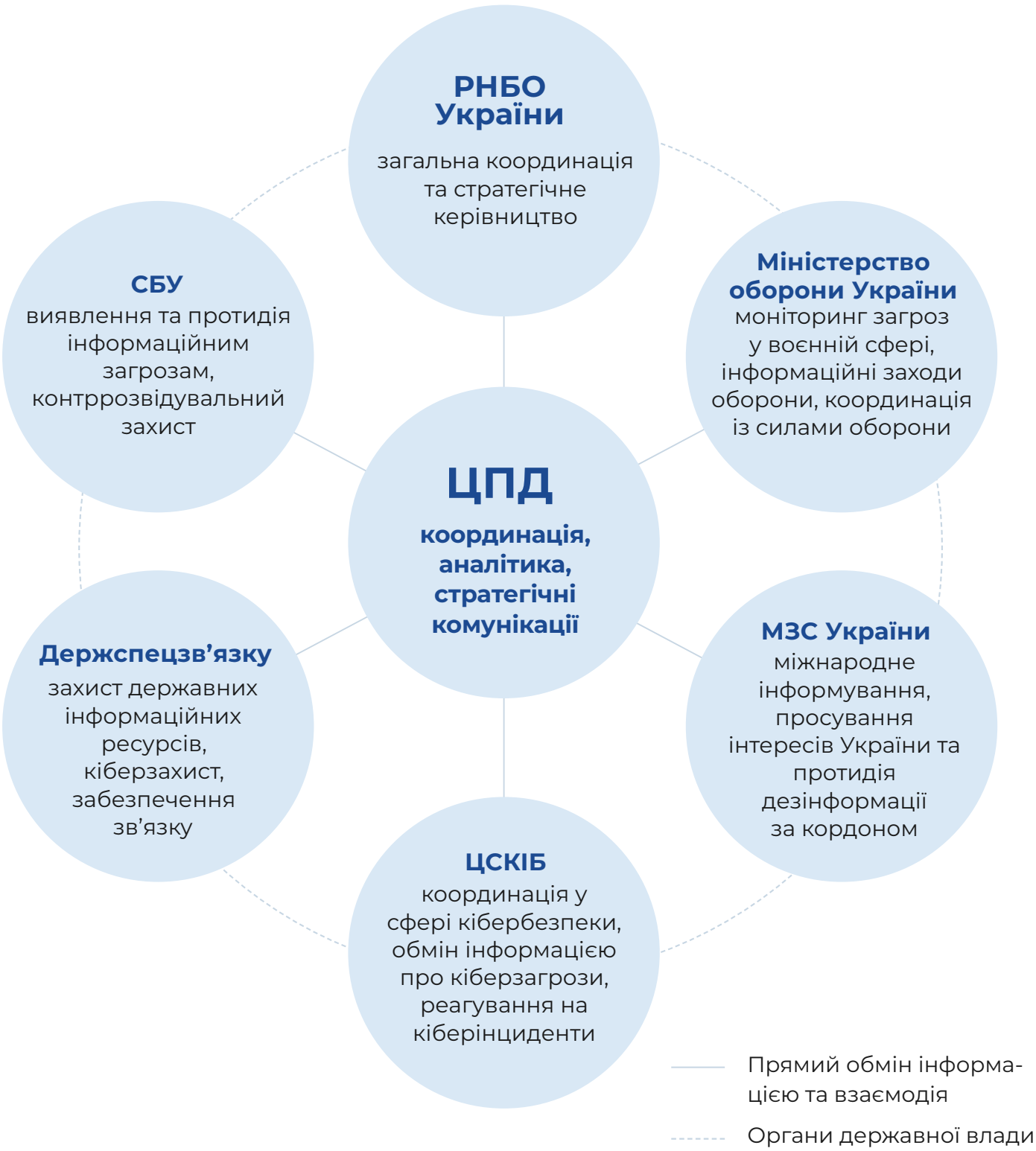
Отже, система моніторингу виконання Стратегії формально функціонувала та забезпечила накопичення значного масиву інформації про діяльність державних

органів, проте не сформувалася як повноцінна система оцінювання, що могла би встановити зв'язок окремих заходів із досягненням стратегічних цілей.

У наступному стратегічному циклі моніторинг доцільно доповнити вимірюваними показниками змін в інформаційному середовищі, безпосередньо пов'язаними з цілями Стратегії. До них можуть належати: динаміка використання різних джерел інформації, рівень довіри до медіа й офіційних джерел, поширеність фактчекінгу, вразливість до інформаційних маніпуляцій, а також загальний рівень медіаграмотності та його розподіл між окремими соціальними й віковими групами. Вихідні значення і цільова динаміка таких показників слід визначити на початку реалізації Стратегії та вимірювати за сталою методологією. Джерелами таких даних можуть бути, зокрема, щорічне дослідження Internews щодо споживання новин і довіри до медіа, що дає змогу простежувати динаміку з 2015 року, та Індекс медіаграмотності українців від ГО «Детектор медіа» — із 2020 року. Результати останнього у 2025 році презентували разом із «Фільтром». Водночас зміни цих показників не можна автоматично приписувати лише реалізації Стратегії, оскільки на них впливають і війна, і трансформація медіасередовища, і інші зовнішні чинники. Тому їх слід використовувати разом із даними про охоплення конкретних заходів, характеристики їхніх цільових аудиторій та оцінювання їхнього безпосереднього впливу (наприклад, через заповнення опитників).

Результати такого оцінювання можуть бути корисні для перегляду заходів, індикаторів, строків і розподілу ресурсів, перетворюючи моніторинг із механізму звітування на інструмент коригування державної політики.

Схема координації органів у сфері інформаційної безпеки



ЦПД — Центр протидії дезінформації

ЦСКІБ — Центр стратегічних комунікацій та інформаційної безпеки

РНБО — Рада національної безпеки і оборони України

СБУ — Служба безпеки України

МЗС — Міністерство закордонних справ України

4. АНАЛІЗ РЕАЛІЗАЦІЇ СТРАТЕГІЧНИХ ЦІЛЕЙ

Зведена таблиця реалізації цілей Стратегії інформаційної безпеки

ЦІЛЬ 1.

Протидія дезінформації та інформаційним операціям, насамперед державі-агресора.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Сформована розгалужена система реагування із залученням ЦПД, ЦСКІБ, СБУ, Держспецзв'язку, МЗС, Міноборони та інших органів.	Процесні показники переважають над результативними.	Створені працездатні механізми виявлення та обмеження інформаційних загроз.
Поряд із моніторингом і підготовкою аналітичних матеріалів застосовані правоохоронні, технічні та регуляторні механізми.	Немає послідовного вимірювання впливу заходів на рівень стійкості суспільства до дезінформації.	Водночас звітність не завжди дозволяє встановити, наскільки ці заходи зменшили поширення дезінформації або підвищили стійкість суспільства до інформаційних загроз.
Розвинено також міжнародний напрям протидії російським інформаційним впливам.	Повторюваність описів окремих заходів і дублювання інформації між різними завданнями, що ускладнює оцінку їхнього індивідуального внеску.	

ЦІЛЬ 2.

Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Виробництво і поширення українського аудіовізуального та книжкового продукту, зокрема переклади творів українських авторів.	Немає показників змін громадянської ідентичності, суспільної згуртованості й довіри до інституцій.	Попри значний обсяг реалізованих культурних та інституційних заходів, оцінити їхній внесок у досягнення стратегічної мети важко, адже немає якісної оцінки досягнутих результатів.
Реалізовані мовно-просвітницькі проєкти й ініціативи у сфері історичної пам'яті.	Звіти здебільшого фіксують лише кількість продуктів і заходів.	Наявна система моніторингу демонструє масштаби діяльності, але не завжди підтверджує її вплив на розвиток культури чи формування громадянської ідентичності.
Затверджений Правопис кримськотатарської мови — довгострокове нормативне підґрунтя для її використання.	У 2025 році через бюджетні обмеження не всі заходи були організовані.	
	Немає єдиної системи оцінювання для численних виконавців.	

ЦІЛЬ 3.

Підвищення рівня медіакультури та медіаграмотності суспільства.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Національний проєкт «Фільтр» і комплекс освітніх продуктів, зокрема Національний тест та Всеукраїнський урок медіаграмотності.	Значна частина заходів має локальний або проєктний характер.	Створена помітна екосистема освітніх і дослідницьких ініціатив.
Сформовані партнерства з освітніми установами, громадськими та міжнародними організаціями	Системне охоплення населення та інтеграція медіаграмотності в освіту недостатньо підтверджені.	Але наявні дані не дозволяють підтвердити безпосередній зв’язок між окремими заходами та змінами суспільних навичок чи визначити динаміку рівня медіакультури та медіаграмотності населення.

ЦІЛЬ 4.

Забезпечення свободи слова та інформації, захист приватного життя і прав журналістів та протидія поширенню незаконного контенту.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Ухвалений Закон №4212-IX запровадив обов'язкові публічні трансляції засідань парламентських комітетів ВРУ та сесій органів місцевого самоврядування.	У звітності немає системних даних про необґрунтовані відмови в доступі до інформації, застосування трискладового тесту й ефективність оскарження.	Реалізація цілі заклала важливий демократичний запобіжник та нормативно-правовий фундамент для євроінтеграції, але на практиці захист журналістів та доступ до інформації суттєво обмежені.
Інтегрований трек протидії юридичному тиску (Anti-SLAPP) до Дорожньої карти з питань верховенства права в межах євроінтеграційних реформ за Кластером 1 «Fundamentals».	Захист журналістів досі недостатньо превентивний, а національні Anti-SLAPP гарантії ще не запроваджені.	Основний розрив полягає у частковій декларативності заходів захисту журналістів замість створення дієвих превентивних процесуальних механізмів.
	Термінологічна невизначеність між «незаконним» та «шкідливим» контентом ускладнює ефективну протидію.	

ЦІЛЬ 5.

Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих і прилеглих до них територіях.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Підтримка мовлення у прифронтових і прикордонних регіонах, відновлення радіотелевізійних станцій із дозволами на тимчасове мовлення.	Поняття інформаційної реінтеграції не визначене. Це ускладнює встановлення чітких меж такої цілі та оцінювання її результативності.	Держава підтримувала інформаційну інфраструктуру та виробництво контенту в умовах війни.
Вироблявся інформаційний контент про ситуацію на окупованих територіях та український спротив.	Показники фіксують кількість дозволів, передавачів і матеріалів — але не фактичний доступ людей з окупованих територій до української інформації, безпечність каналів зв'язку або довіру до контенту.	Водночас наявні дані не дозволяють встановити, наскільки громадяни на окупованих територіях реально зберегли або відновили зв'язок із українським інформаційним простором.
Проводилася міжнародна комунікація щодо статусу тимчасово окупованих територій.		

ЦІЛЬ 6.

Створення ефективної системи стратегічних комунікацій.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Створені працездатні секторальні механізми підготовки фахівців, координації повідомлень та кризових комунікацій.	Секторальні механізми недостатньо об'єднані в єдину загальнодержавну систему.	Сформовані функціональні елементи стратегічних комунікацій, але вони не інтегровані в інституційно сталу систему.
Значного масштабу досягли іномовлення і міжнародні комунікації.	Горизонтальна координація досі недостатня, регіональні спроможності нерівномірні, бракує фахівців.	Звітність підтверджує заходи щодо навчань, координації та поширення контенту, проте недостатньо відображає їхній вплив на узгодженість державних комунікацій і визначені аудиторії.
Розширене виробництво іншомовного контенту та його поширення через закордонні мережі.	Взаємодія з ОГС і медіа та частина координаційних практик досі лишаються проєктними або залежними від персональної ініціативи.	

ЦІЛЬ 7.

Розвиток інформаційного суспільства та підвищення рівня культури діалогу.

Позитивні аспекти реалізації	Потребує покращення	Оцінка результату і впливу
Найбільш відчутних результатів досягнуто у розвитку інфраструктури мовлення. Наприклад, було розгорнуто мережу МХ-7, що станом на кінець 2025 року налічувала 167 передавачів і охоплювала понад 90% території України.	Реформа системи мовлення територіальних громад просувалася повільно. Наприклад, за підсумками 2025 року реорганізацію завершило лише п’ять компаній.	Чітких результатів досягнуто в розвитку інфраструктури мовлення та цифрових рішень.
Реалізовувалися проєкти з модернізації захищених інформаційно-комунікаційних систем.	Підвищення рівня культури діалогу не було належно операціоналізовано: План не визначив змісту цього поняття та не передбачив якісних показників оцінювання.	Водночас наявні звітні дані не дають змоги оцінити, наскільки ці результати розширили фактичний доступ цільових аудиторій до українського контенту.
Суспільний мовник розвивав дитячий і підлітковий контент, зокрема запустив медіасервіс «БРОБАКС».	Не всі заходи виконані. Так, спеціальний фонд для фінансування виробництва дитячих фільмів не створено.	Суспільно-комунікативні складові цілі — місцеве мовлення, підтримка дитячого контенту, культура діалогу — реалізовані частково або недостатньо вимірювані.

Детальний розбір реалізації всіх стратегічних цілей стратегії інформаційної безпеки ви можете прочитати на нашому сайті за посиланням –

https://cedem.org.ua/analytics/strategiya-infobezpeky-analityka/

ВИСНОВКИ

Стратегія інформаційної безпеки 2021 року сформувала широку рамку державної політики у цій сфері. Її сильною стороною стало комплексне бачення інформаційної безпеки, що охоплювало не лише протидію дезінформації, а й розвиток української культури, медіаграмотність, забезпечення інформаційних прав, реінтеграцію тимчасово окупованих територій, стратегічні комунікації та інформаційну інфраструктуру.

Водночас є і важливий нюанс: ця Стратегія затверджена до початку повномасштабного вторгнення. План заходів із її реалізації, ухвалений у березні 2023 року, вже враховував окремі потреби, зумовлені новим етапом збройної агресії, чим певною мірою адаптував реалізацію Стратегії до змінених умов. Однак пізніше ухвалення Плану не могло повністю компенсувати відсутність змістовного перегляду самої Стратегії, зокрема її оцінку загроз, стратегічні пріоритети й загальну логіку, сформовану в безпековому середовищі до 24 лютого 2022 року.

Стратегія визначала напрями державної політики, однак не формувала цілісної логіки переходу від загроз до очікуваних суспільних змін. Частина стратегічних цілей і завдань була сформульована надто широко, окремі положення дублювалися, а ключові поняття — зокрема «інформаційна реінтеграція», «культура діалогу», «інформаційна стійкість» та «ефективна система стратегічних комунікацій» — не були операціоналізовані. Через змістове перетинання окремих цілей про однакові заходи могли одночасно звітувати за різними цілями, а формальне виконання окремих завдань не завжди свідчило про досягнення їхнього змістовного результату.

План заходів визначив виконавців, строки та індикатори, але не всі завдання Стратегії були належно конкретизовані. В окремих випадках зв'язок між стратегічною ціллю, завданням, заходом та індикатором був слабким чи опосередкованим. Частина індикаторів вимірювала кількість проведених заходів, консультацій, інформаційних матеріалів чи виданих дозволів — але не зміни у доступі до інформації, довірі, медіаграмотності, стійкості до дезінформації або якості державних комунікацій. Отже, План дозволяв відстежувати переважно адміністративну активність, але значно меншою мірою — результативність і вплив заходів на суспільство.

Найкраще задокументовані безпосередні результати спостерігалися у напрямах, де завдання передбачали створення конкретного продукту чи інфраструктурну зміну. Наприклад, окремі заходи із підтримки мовлення у прикордонних і прифронтових районах, виробництво українського культурного й інформаційного контенту, розвиток іномовлення, реалізація масштабних міжнародних комунікаційних кампаній, а також створення освітніх продуктів у межах проєкту «Фільтр». У цих напрямах офіційна звітність дозволяє встановити принаймні наявність конкретних безпосередніх результатів, хоча їхній внесок у досягнення стратегічних цілей і довгостроковий суспільний вплив не завжди були належно виміряні.

Менш результативними або недостатньо вимірюваними лишилися напрями, пов'язані зі складними суспільними й інституційними змінами. Звітність не дозволяє достовірно оцінити, наскільки державні заходи зменшили вразливість населен-

ня до дезінформації, зміцнили громадянську ідентичність, поліпшили дотримання інформаційних прав, забезпечили інформаційну реінтеграцію громадян на тимчасово окупованих територіях або підвищили культуру діалогу. Водночас відсутність належних показників не означає відсутність позитивного впливу, але й не дозволяє його обґрунтовано підтвердити.

Повільно просувалася реформа мовлення територіальних громад, не було створено передбаченого Планом спеціального фонду підтримки дитячого контенту, а захист журналістів і запобігання SLAPP-позовам (підготовка анти-SLAPP законодавства затягнулася) не набули системного превентивного характеру.

Виконання Стратегії продемонструвало адаптивність державних органів в умовах повномасштабної війни. Були розширені кризові та міжнародні комунікації, запроваджені нові формати аналітики, навчання і взаємодії, підтримане мовлення на територіях із підвищеним ризиком інформаційної ізоляції. Однак така адаптація часто відбувалася через практичні рішення окремих органів, міжнародні проєкти або персональну координацію, а не через формальний перегляд Стратегії та Плану. Хоч це і допомогло швидко реагувати на кризові ситуації, але не завжди забезпечувало інституційну сталість створених механізмів.

Інституційна система реалізації Стратегії залишалася фрагментованою. Окремі органи сформували власні спроможності у сфері моніторингу, стратегічних комунікацій, протидії дезінформації та кризового реагування, проте вони не були повністю інтегровані в єдину систему з чітко розподіленими функціями, порядком обміну інформацією та механізмом вирішення міжвідомчих розбіжностей. Особливо помітними були нерівномірність регіональних спроможностей — брак підготовлених фахівців і залежність частини ініціатив від міжнародної технічної допомоги та громадянського суспільства.

Окремий системний недолік — відсутність цілісного підходу до взаємодії держави з великими цифровими платформами. Стратегія визнавала значення соцмереж у поширенні інформаційних загроз, але не визначила відповідальні органи, процедури співпраці, вимоги до прозорості платформ чи гарантії захисту свободи слова і приватності. Практика точкового обмеження доступу до окремих ресурсів і незаконного контенту або координованих ворожих операцій може бути необхідною, однак не відповідає системному характеру алгоритмічного поширення інформації. Відсутність чіткого розмежування між незаконним і законним, але потенційно шкідливим контентом додатково створює ризик непропорційного втручання у свободу слова. Окремими складовими наступного стратегічного циклу мають стати системне врахування ризиків, пов'язаних із генеративним штучним інтелектом, синтетичним контентом, алгоритмічними системами поширення інформації, а також поступове наближення українського законодавства й інституційної системи до DSA.

Система звітування забезпечила накопичення значного обсягу інформації, проте не стала повноцінним механізмом оцінювання політики. Дані переважно від виконавців, зміни у структурі звітів, відсутні чи неповні відомості за попередні роки у наступних звітах, а окремі результати повторювалися в межах різних завдань. Тому за звітністю складно простежити сукупний прогрес за весь період реалізації Стра-

тегії або відокремити внесок конкретного заходу від ширших процесів, зумовлених війною, законодавчими реформами чи діяльністю міжнародних партнерів.

Отже, Стратегія стала корисною основою для консолідації державної діяльності й забезпечила низку конкретних результатів. Водночас її реалізація виявила розрив між широкими стратегічними намірами та здатністю Плану заходів перетворити їх на вимірювану, скоординовану й ресурсно забезпечену політику.

Головним завданням наступного стратегічного циклу має стати не механічне розширення переліку загроз і заходів, а формування цілісної, адаптивної та заснованої на правах людини системи інформаційної безпеки. У ній кожну загрозу слід пов'язати з конкретною ціллю, відповідальним суб'єктом, необхідними ресурсами, показниками безпосереднього результату і довгострокового впливу та гарантіями дотримання прав людини. Нова Стратегія має також передбачати регулярний перегляд оцінки загроз, інституціоналізовану взаємодію з громадянським суспільством, медіа, дослідниками та цифровими платформами, а також поступову підготовку законодавства й інституцій до наближення України до стандартів ЄС в інформаційній політиці.

СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 2021-2025 РОКІВ:

ОЦІНКА РЕАЛІЗАЦІЇ

HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА