HEINRICH BÖLL STIFTUNG
КИЇВ

ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА

РЕКОМЕНДАЦІЇ

ЩОДО ПІДГОТОВКИ НОВОЇ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

та Плану заходів



РЕКОМЕНДАЦІЇ ЩОДО ПІДГОТОВКИ НОВОЇ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ТА ПЛАНУ ЗАХОДІВ

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

Рекомендації 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

ЗМІСТ

Вступ 5

Виклики попереднього циклу 6

Ключові рекомендації 7

РІВЕНЬ 1. СИСТЕМНІ РЕКОМЕНДАЦІЇ 9

Рекомендація 1.1. Використати актуалізацію Стратегії національної безпеки для оновлення її інформаційної складової 10

Рекомендація 1.2. Доопрацювати й ухвалити Стратегію інформаційної безпеки і План заходів на основі оновленої Стратегії національної безпеки 11

Рекомендація 1.3. Узгодити Стратегію з іншими документами державної політики 11

Рекомендація 1.4. Чітко розподілити відповідальність за узгодженість реалізації Стратегії 12

Рекомендація 1.5. Створити публічний реєстр стратегічних документів 12

Рекомендація 1.6. Спиратися на узгоджені державні позиції як основу для урядових комунікацій 13

РІВЕНЬ 2. ІНСТИТУЦІЙНІ РЕКОМЕНДАЦІЇ 14

Рекомендація 2.1. Посилити спроможність СКМУ координувати урядові комунікації 15

Рекомендація 2.2. Закріпити запобіжники для свободи слова та незалежності медіа 16

Рекомендація 2.3. Посилити оперативну міжвідомчу координацію 16

Рекомендація 2.4. Закріпити партнерство із громадянським суспільством на всіх етапах 17

Рекомендація 2.5. Забезпечити інституційну сталість урядових комунікацій 18

РІВЕНЬ 3. ОПЕРАЦІЙНІ РЕКОМЕНДАЦІЇ 19

Рекомендація 3.1. Чітко формулювати стратегічні завдання, заходи та індикатори виконання 20

Рекомендація 3.2. Забезпечити прозоре та деталізоване планування ресурсів для реалізації Плану заходів 20

Рекомендація 3.3. Вимірювати зміни, а не лише виконані дії 21

Рекомендація 3.4. Щорічно оцінювати ситуацію та за потреби переглядати План або Стратегію 22

РІВЕНЬ 4. ПРІОРИТЕТНІ НАПРЯМИ **23**

Рекомендація 4.1. Від реагування — до запобігання 24

Рекомендація 4.2. Враховувати потреби різних аудиторій 24

Рекомендація 4.3. Розвивати системну взаємодію із цифровими платформами 25

Рекомендація 4.4. Розвивати медіаграмотність як основу стійкості суспільства 25

Рекомендація 4.5. Виробити комплексну політику щодо тимчасово окупованих територій і відновлення інформаційного простору після деокупації 26

Рекомендація 4.6. Захищати свободу слова та журналістів 26

Висновки **27**

ВСТУП

В умовах повномасштабної війни інформаційна безпека стала однією з умов стійкості держави і суспільства, а Стратегія інформаційної безпеки (далі — Стратегія) визначає, як саме держава захищає інформаційний простір і водночас зберігає свободу слова.

У 2026 році Центр демократії та верховенства права (ЦЕДЕМ) провів дослідження «Стратегія інформаційної безпеки 2021–2025 років: оцінка реалізації». Воно показало, що Стратегія, термін якої сплив у 2025-му році, дала низку конкретних позитивних результатів. Водночас її реалізація виявила розрив між широкими стратегічними намірами та здатністю Плану заходів перетворити їх на вимірювану, скоординовану й забезпечену ресурсами політику.

Мета цього документа — надати рекомендації для нового циклу політики інформаційної безпеки — як до майбутньої Стратегії та її місця в системі державного планування, так і до майбутнього Плану заходів із її реалізації. Із 19 листопада по 3 грудня 2025 року тривало громадське обговорення проєкту Стратегії та пояснювальної записки, а у жовтні 2026 року його представили публічно.

Частина викликів, виявлених у попередньому циклі, має системний характер: вони стосуються не лише конкретно Стратегії, а й загалом системи державного стратегічного планування, тож їх доцільно розглядати в ширшому контексті реформування цієї системи. Інші аспекти безпосередньо стосуються реалізації Стратегії, і їх можна врахувати під час розробки Плану заходів.

Указом Президента України від 26 жовтня 2026 року №1066/2026 введено у дію рішення РНБО «Про актуалізацію Стратегії національної безпеки України». Апарату РНБО спільно з Національним інститутом стратегічних досліджень доручено, із залученням заінтересованих державних органів, інституцій громадянського суспільства та іноземних експертів протягом трьох місяців підготувати пропозиції змін до документа. За результатами цього процесу мають бути визначені й завдання щодо підготовки та ухвалення галузевих стратегій. Так, у 2020 році рішення РНБО, введене в дію Указом Президента №392/2020, передбачало подання на розгляд РНБО проєкту Стратегії інформаційної безпеки протягом шести місяців. Оскільки галузева Стратегія розвиватиме засади документа вищого рівня, частину рекомендацій доцільно врахувати вже під час актуалізації Стратегії національної безпеки. Це допоможе закласти обґрунтовані пріоритети інформаційної безпеки та забезпечити їх послідовне відображення у новій Стратегії та Плані заходів.

В основі даних рекомендацій — висновки дослідження ЦЕДЕМ; аналіз офіційних звітів про виконання Плану заходів за 2023–2025 роки; матеріали трьох експертних обговорень, які ЦЕДЕМ провів із представниками громадянського суспільства, медіа та незалежними експертами; а також на міжнародних дослідженнях і оцінках, зокрема ОЕСР та SIGMA, соціологічних даних про споживання медіа та медіаграмотність і досвіді інших країн.

ВИКЛИКИ ПОПЕРЕДНЬОГО ЦИКЛУ

Нижче описано вісім наскрізних викликів, що стосуються системи реалізації Стратегії загалом.

1. Слабкий зв'язок Стратегії з іншими державними документами. Стратегію ухвалили на основі Стратегії національної безпеки 2020 року, ще до повномасштабного вторгнення, і її логіка загроз згодом застаріла. Частину питань, важливих для інформаційної безпеки, регулюють інші документи, а частина цілей сформульована надто широко, щоб на їх основі реалізувати вимірювані заходи.

2. Фрагментованість інституційної системи та недостатня визначеність координаційних механізмів. Розподіл функцій між органами існував, але процедури їх горизонтальної взаємодії не були чітко прописані. Дієві механізми координації сформувалися здебільшого в окремих секторах і часто залежали від конкретних посадовців.

3. Потреба в узгоджених державних позиціях і кращому розумінні аудиторій. У деяких темах, зокрема щодо окупованих територій, труднощі виникали не так у комунікації, як у відсутності чітко сформованої політики. Водночас різні групи населення мають різні джерела інформації та рівень медіаграмотності, тому комунікація має спиратися на їхні потреби.

4. Недостатня деталізація фінансового забезпечення. Загальні положення про фінансування Стратегії та Плану заходів не супроводжувалися деталізацією орієнтовних витрат і джерел фінансування кожного заходу, що ускладнювало оцінку необхідних ресурсів для їх виконання.

5. Звітність про виконану роботу, а не про досягнуті цілі. Моніторинг фіксував переважно проведені заходи, а не їх вплив на стан інформаційної безпеки. Вже наявні регулярні дослідження медіаспоживання і медіаграмотності (від «Інтерньюз-Україна», «Детектор медіа» та інших) для оцінювання Стратегії майже не використовували.

6. Обмежене й недостатньо формалізоване залучення громадянського суспільства. Співпраця з громадськими організаціями була широкою, але здебільшого проєктною. У формуванні політики та оцінюванні результатів участь організацій була обмеженою, і прозорих правил їх залучення не було прописано.

7. Відсутність цілісного підходу до цифрових платформ. Стратегія не визначала, хто і як координує взаємодію держави із платформами. Контакти з ними залишалися ситуативними і недостатньо прозорими, а месенджери та генеративний ШІ за останні роки стали провідними каналами поширення інформаційних загроз.

8. Відсутність механізму регулярного перегляду. Після повномасштабного вторгнення План частково врахував нові умови, але змістовного перегляду самої Стратегії не відбулося. Адаптація до нових викликів відбувалася неформально, через рішення окремих органів і окремі проєкти.

КЛЮЧОВІ РЕКОМЕНДАЦІЇ

1. Оновити інформаційну складову Стратегії національної безпеки. Під час її актуалізації важливо визначити актуальні загрози і механізм їх перегляду, а також оновити пріоритети державної політики та принципи захисту інформаційного простору, які надалі розвиватиме нова Стратегія інформаційної безпеки.

2. Забезпечити узгодженість Стратегії інформаційної безпеки з іншими стратегічними документами та її своєчасне ухвалення. Доопрацювання Стратегії має враховувати оновлені положення Стратегії національної безпеки та суміжних державних документів для уникнення суперечностей, дублювання і прогалин. План заходів доцільно готувати паралельно, забезпечивши послідовність ухвалення документів і своєчасний початок їх реалізації.

3. Сформувати цілісну систему координації виконання Стратегії та посилити роль Секретаріату Кабінету Міністрів України (СКМУ) в координації урядових комунікацій. Варто об'єднати вже дієві секторальні механізми в цілісну міжвідомчу систему з чіткими правилами взаємодії, повноваженнями координатора та спільними інструментами планування, зберігши запобіжники для незалежності медіа й громадянського суспільства. Для координації урядових комунікацій слід забезпечити СКМУ належними повноваженнями й ресурсами.

4. Виробляти узгоджену позицію відомств із ключових питань до виходу з публічними заявами. У чутливих темах, зокрема щодо тимчасово окупованих територій, органи влади мають спершу узгодити позицію між собою, а потім виходити з нею до суспільства, щоб держава говорила одним голосом і не залишала простору для маніпуляцій противника через суперечливі повідомлення.

5. Узагальнити й оприлюднити інформацію про сукупну вартість і джерела фінансування кожного заходу Плану. Це дасть чітке розуміння, які заходи забезпечені ресурсами, і допоможе визначити додаткові фінансові потреби. Оцінки витрат варто щорічно уточнювати, а у звітах — зіставляти заплановані й фактичні витрати.

6. Вимірювати не лише виконану роботу, а і яких цілей вона досягла. Для кожного заходу варто визначити, що має змінитися для аудиторії та за яким показником це можна буде вирахувати, за можливості, на основі наявних регулярних досліджень.

7. Залучати громадянське суспільство, науковців і бізнес на всіх етапах. Участь має охоплювати весь цикл, від підготовки Стратегії — до перегляду Плану, за прозорими правилами та з обґрунтованою відповіддю на кожну пропозицію.

8. Вибудувати системну взаємодію із цифровими платформами з гарантіями дотримання прав людини. Для цього потрібен відповідальний орган, зрозумілі процедури звернень, публічна звітність і поступове наближення до підходів ЄС, зокрема Акта про цифрові послуги.

9. Щороку оцінювати ситуацію з реалізацією та за потреби оновлювати План заходів. Стратегія — довгостроковий документ, тому переглядати її доцільно лише в разі критично важливих змін, але оновлювати План заходів можна і потрібно для адаптації до нових викликів мінливого інформаційного середовища.

Наведені ключові рекомендації окреслюють головні напрями змін. Нижче вони розкриті детальніше і згруповані за чотирма рівнями.

Системний рівень стосується місця Стратегії в державній політиці: її зв'язку з іншими документами, зокрема зі Стратегією національної безпеки, яку нині актуалізують, а також із бюджетом.

Інституційний рівень охоплює координацію між органами влади, запобіжники для свободи слова та партнерство із громадянським суспільством.

Операційний рівень визначає власне План заходів: як краще формулювати заходи, забезпечувати їх ресурсами, вимірювати результати і переглядати План.

Рівень пріоритетних напрямів окреслює, на чому варто зосередити зусилля в наступному циклі. Частина рекомендацій виходить за межі Плану заходів і стосується ширшої системи державного планування, інші можна врахувати безпосередньо під час розробки Плану. Кожна рекомендація спирається на висновки дослідження ЦЕДЕМ, міжнародні дослідження та пропозиції учасників експертних обговорень.

РІВЕНЬ 1.
СИСТЕМНІ РЕКОМЕНДАЦІЇ



Рекомендації цього рівня стосуються місця Стратегії в загальній системі державного планування. Від того, наскільки змістовно Стратегія пов’язана зі Стратегією національної безпеки, суміжними документами та бюджетом, залежить, чи стане вона ефективним робочим інструментом. Актуалізація Стратегії національної безпеки, розпочата у жовтні 2026 року, створює для цього сприятливу нагоду: спершу оновити інформаційну складову документа вищого рівня, а потім на її основі ухвалити Стратегію інформаційної безпеки.

1.1. Використати актуалізацію Стратегії національної безпеки для оновлення її інформаційної складової

Стратегія інформаційної безпеки розробляється на виконання Стратегії національної безпеки, тому її актуалізація визначить рамку для нової Стратегії інформаційної безпеки. Документ вищого рівня має врахувати досвід попереднього циклу реалізації Стратегії інформаційної безпеки та зміни інформаційного середовища, визначити актуальні загрози і механізм їх перегляду, оновити пріоритети державної політики та принципи захисту інформаційного простору з дотриманням прав людини. Неповнота чи суперечливість цих положень може ускладнити подальше галузеве планування.

Корисний орієнтир — досвід країн, що системно протидіють російським інформаційним операціям. Естонія інтегрувала інформаційну безпеку безпосередньо в Концепцію національної безпеки і пов'язала її з психологічною обороною і стійкістю суспільства. Швеція у 2026 році представила стратегію психологічної оборони як частину системи тотальної оборони. В обох випадках інформаційна безпека не існує як окремий напрям: її цілі, відповідальні органи й ресурси чітко узгоджені із загальною безпековою політикою держави і зусиллями для забезпечення стійкості суспільства. Для України це аргумент на користь реального змістовного зв’язку Стратегії інформаційної безпеки зі Стратегією національної безпеки, зокрема під час актуалізації останньої.

Рекомендовано оновити оцінку інформаційних загроз із урахуванням досвіду повномасштабної війни, розвитку генеративного ШІ та ролі цифрових платформ; розвинути положення щодо розвитку системи урядових стратегічних комунікацій, взаємодії із цифровими платформами та зміцнення суспільної стійкості; передбачити належні гарантії свободи вираження поглядів і доступу до інформації.

У рішенні щодо актуалізації Стратегії національної безпеки можна, як і в попередньому стратегічному циклі, визначити завдання, відповідальних за доопрацювання Стратегії інформаційної безпеки і строки її подання на розгляд.

1.2. Доопрацювати й ухвалити Стратегію інформаційної безпеки і План заходів на основі оновленої Стратегії національної безпеки

Оскільки Стратегія інформаційної безпеки покликана розвивати положення документа вищого рівня, її доцільно ухвалювати вже після актуалізації Стратегії національної безпеки. Підготовлений проєкт Стратегії інформаційної безпеки при цьому не втрачає цінності: його варто доопрацювати з урахуванням оновленої оцінки загроз і засад державної політики. Щоб уникнути тривалої паузи між прийняттям документів, доопрацювання проєкту можна вести паралельно з підготовкою пропозицій щодо актуалізації інформаційної складової Стратегії національної безпеки.

Так само важливо не допустити розриву між Стратегією інформаційної безпеки і Планом заходів. У попередньому циклі між ухваленням Стратегії (грудень 2021 року) і Плану (березень 2023 року) минуло більше року. Рекомендовано розпочати підготовку Плану заходів паралельно зі Стратегією і залучати до його розробки представників громадянського суспільства.

Такий підхід допоможе забезпечити своєчасне ухвалення галузевої Стратегії після оновлення документа вищого рівня та уникнути тривалої перерви між її ухваленням і затвердженням Плану заходів.

1.3. Узгодити Стратегію з іншими документами державної політики

Стратегія інформаційної безпеки виходить зі Стратегії національної безпеки і перетинається з іншими документами: стратегіями кібербезпеки та зовнішньополітичної діяльності, Концепцією забезпечення національної системи стійкості, політикою щодо реінтеграції та іншими. Якщо ці документи не узгоджені, виникають дублювання чи прогалини. Це загальна проблема державного планування: Організація економічного співробітництва та розвитку (ОЕСР) рекомендує Україні визначити чітку ієрархію планувальних документів, аби було зрозуміло, який документ визначає пріоритети для інших.

Рекомендовано:

- відобразити у Стратегії або пояснювальних матеріалах до неї, які питання вона регулює, а які залишено іншим документам;
- для заходів Плану на перетині кількох сфер зазначати пов'язаний документ і відповідальний за нього орган.

1.4. Чітко розподілити відповідальність за узгодженість реалізації Стратегії

Під час виконання заходи різних стратегій неминуче перетинаються. Медіаграмотність стосується і Стратегії інформаційної безпеки, і освітньої політики. Комунікація із жителями окупованих територій стосується також політики реінтеграції, а захист медіа від кібератак — Стратегії кібербезпеки. Щоб органи діяли злагоджено і не залишали прогалин, потрібно чітко визначити, хто відповідає за узгодженість на різних рівнях.

У попередньому циклі координаційні ролі були визначені розмито. Стратегія покладала координацію у сфері інформаційної безпеки на РНБО, а роботу міністерств — на Кабінет Міністрів. 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.

Рекомендовано у новій Стратегії чітко визначити, як розподіляються ролі між СКМУ, РНБО та профільним міністерством, а також як ці органи взаємодіють між собою. Зокрема варто визначити, хто забезпечує узгодженість Стратегії з іншими урядовими та безпековими документами і хто координує виконання Плану, а також якими повноваженнями для цього наділений кожен із цих органів. ОЕСР рекомендує посилити координаційну роль СКМУ у стратегічному плануванні.

1.5. Узгодити Стратегію з іншими документами державної політики

В Україні немає єдиного відкритого реєстру, де можна побачити всі чинні стратегії, їхній статус і взаємозв'язки між ними. Через це складно зрозуміти, які документи діють, хто за них відповідає і де вони перетинаються. Все це ускладнює роботу і самих органів влади, і громадськості, яка стежить за виконанням.

Рекомендовано створити такий реєстр на загальнодержавному рівні. Для кожного документа в ньому варто вказувати статус, відповідальний орган, строк дії, пов'язані документи, а також план заходів і звіти про його виконання.

1.6. Спиратися на узгоджені державні позиції як основу для урядових комунікацій

Урядові комунікації пояснюють суспільству державну політику, але вони не можуть замінити саму політику там, де вона ще не сформована. Якщо держава не має чіткої позиції з певного питання, комунікаційники не можуть пояснити її громадянам, а противник може легко цим скористатися, заповнюючи цю порожнечу власними наративами.

Показовий приклад — питання тимчасово окупованих територій, де ворог поширює чутки, ніби після деокупації українська влада переслідуватиме всіх, хто отримав російський паспорт. Шукати контраргументи на такі чутки складно, поки немає узгодженої державної позиції щодо взаємодії з людьми на окупованих територіях. Як наголошували учасники експертних обговорень, організованих ЦЕДЕМ, у таких випадках проблема полягає не так у комунікації, як у відсутності чітко визначеної державної позиції.

Тому пропонуємо низку рекомендацій щодо цих питань.

- Розробити механізм регулярного визначення тем і питань, щодо яких бракує узгодженої державної позиції, та органів, відповідальних за її вироблення. Такі теми можна виявляти під час моніторингу інформаційних кампаній противника та щорічної оцінки ситуації (див. рекомендацію 3.4), а перелік оновлювати в міру появи нових викликів. Серед тем, які потребують уваги вже зараз, — ставлення до громадян на окупованих територіях, колаборація, реінтеграція тощо.
- Залучати фахівців із комунікацій до підготовки рішень від самого початку, а не лише на етапі їх оприлюднення.
- Доводити узгоджені позиції до всіх органів, які комунікують із відповідними аудиторіями, щоб вони говорили одним голосом від імені держави.
- Переглядати позиції, коли змінюється ситуація, і своєчасно повідомляти про це суспільству.

РІВЕНЬ 2.
ІНСТИТУЦІЙНІ РЕКОМЕНДАЦІЇ



Рекомендації цього рівня стосуються того, як органи влади взаємодіють між собою та із суспільством. Попередній цикл показав, що ефективна співпраця можлива, але вона часто трималася на окремих людях і секторальних ініціативах. Щоб взаємодія стала системною, потрібні чіткі правила координації, запобіжники від утиску свободи слова й атак на незалежні медіа, а також постійне партнерство із громадянським суспільством.

2.1. Посилити спроможність СКМУ координувати урядові комунікації

Під час експертних зустрічей, організованих ЦЕДЕМ, неодноразово лунала теза про потребу посилити комунікаційну та координаційну роль СКМУ. Окремі міністерства повинні мати розвинені спроможності для комунікації своїх політичних пріоритетів, однак узгодження цих комунікацій щодо спільних урядових пріоритетів потребує відповідальності на рівні центру уряду. Такий підхід відповідає принципам державного управління SIGMA, які передбачають центральну координацію урядових комунікацій та міжвідомчі механізми її здійснення.

У наступному стратегічному циклі рекомендовано передбачити можливість посилення відповідної функції СКМУ: уточнення повноважень відповідального підрозділу та посадових осіб, забезпечення належних кадрових і фінансових ресурсів, а також визначення порядку взаємодії з комунікаційними підрозділами міністерств. Ця функція має охоплювати спільне планування комунікацій щодо урядових пріоритетів, узгодження дій із питань, що належать до компетенції кількох органів, та координацію кризових комунікацій.

Для визначення пріоритетних напрямів посилення комунікаційної спроможності СКМУ варто звернути увагу на п’ять складових, які пропонує SIGMA:

1) становлення дієвих міжвідомчих механізмів для координації урядових комунікацій;
2) наявність спільної комунікаційної стратегії, виконання якої координується центром уряду;
3) збір та аналіз інформації про суспільні настрої та потреби;
4) узгодження цифрових комунікацій;
5) оцінка впливу урядових комунікацій.

Координацію урядових комунікацій варто забезпечувати силами постійної команди держслужбовців, щоб їхня робота зберігала послідовність у разі зміни уряду або його політичних радників. Донорська підтримка може посприяти цій спроможності, проте необхідно заздалегідь визначати, як виконуватимуться відповідні функції після завершення проєктів. Показовий приклад Молдови: SIGMA зазначає, що значна частина фахівців із комунікацій працює як зовнішні підрядники, фінансовані донорами, що створює ризики для сталості роботи. Тому залучення міжнародної допомоги доцільно поєднувати зі зміцненням штатної команди, передаванням їй напрацьованих інструментів і забезпеченням фінансування постійних функцій.

2.2. Закріпити запобіжники для свободи слова та незалежності медіа

Більшість учасників експертних обговорень загалом підтримувала посилення координації урядових комунікацій СКМУ, але водночас наголошувала на ризиках можливої цензури. Що більше повноважень матиме координатор, то важливіші запобіжники.

Рекомендовано передбачити три групи запобіжників.

- **Урядові комунікації мають бути відокремлені від політичних.** SIGMA рекомендує Україні забезпечити відокремлення публічної комунікації від політичних меседжів. Це означає, що державні ресурси урядових комунікацій мають служити інформуванню суспільства про державну політику та захисту від загроз, а не підтримці позиції окремих політичних сил чи посадовців.
- **Рекомендації для недержавних учасників інформаційного простору щодо комунікаційних меседжів повинні мати дорадчий характер.** Держава може готувати для медіа, громадських організацій і лідерів думок аналітику про загрози та поради щодо комунікації на чутливі теми — це корисна практика. Водночас експерти застерігали, що такі поради не мають перетворюватися на обов'язкові вказівки, що і як повідомляти. У Плані доцільно прямо зазначити, що такі матеріали — дорадчі й не обмежують редакційної незалежності медіа.
- **Протидія незаконному контенту має бути прозорою.** Державні органи досить часто звертаються до платформ із проханням видалити певний контент або заблокувати облікові записи. Однак звіти не пояснюють, на якій підставі це робиться і за якими критеріями. Варто прописати, які органи і на яких підставах надсилають звернення до платформ, за якими критеріями, а також публікувати узагальнену статистику таких звернень. Прозорість не послаблює безпеку, а зміцнює довіру до дій держави.

2.3. Посилити оперативну міжвідомчу координацію

У попередньому циклі механізм міжвідомчої координації вважався створеним уже тоді, коли його розробили на папері. Недостатньо уваги приділялося ефективності де-факто створених механізмів. Рекомендовано конкретизувати порядок взаємодії органів під час виконання Плану заходів, спираючись на наявні практики і досвід координаційних груп у системах МВС, Міноборони та МЗС. Такий порядок має визначати відповідальних контактних осіб, формати й періодичність планових нарад, канали оперативного зв'язку, а також правила обміну аналітикою про інформаційні загрози та кампанії противника.

Окремо слід визначити порядок взаємодії у кризових ситуаціях: хто ініціює реагування, які органи долучаються, хто узгоджує спільну позицію та хто відповідає за її публічне пояснення. Важливо встановити строки реагування і порядок вирішення розбіжностей, аби міжвідомчі погодження не затримували необхідні дії. Для поточної роботи варто узгодити формат обміну інформацією про виконання Плану, зокрема про затримки, перешкоди і питання, що потребують спільного рішення.

Одним із інструментів планування може бути спільний комунікаційний календар, у якому органи заздалегідь зазначають ключові оголошення та кампанії. SIGMA наводить такий підхід як спосіб узгоджувати комунікаційну діяльність різних міністерств («if it isn't in the calendar / on the grid, it can't be communicated»). Для його практичного використання доцільно визначити відповідального за ведення календаря, порядок його оновлення та внесення термінових змін.

2.4. Закріпити партнерство із громадянським суспільством на всіх етапах

Українські громадські організації, незалежні медіа та фактчекери мають значний досвід у протидії дезінформації та розвитку медіаграмотності. За словами експертів, вони готові до співпраці, але чекають системнішого залучення з боку держави. Для цього рекомендовано кілька кроків.

- Розробити порядок громадських консультацій для всього циклу: від підготовки Стратегії і Плану — до моніторингу й перегляду. У ньому варто прописати, хто може долучитися, як подавати пропозиції і як орган влади пояснює їх врахування чи відхилення.
- Створити відкриту мапу суб'єктів у сфері інформаційної безпеки: щоб залучати організації системно, держава має знати, хто і чим займається у цій сфері. У галузі медіаграмотності подібний крок уже зроблений: на запит Мінкульту підготовлене дослідження ринку медіаграмотності. Доцільно поширити цей підхід на всю сферу інформаційної безпеки та створити відкриту мапу суб'єктів, що охоплює наявні громадські організації, незалежні медіа, фактчекерів, академічні та дослідницькі установи, а також бізнес, зокрема телекомунікаційний і технологічний сектори. Ця мапа повинна регулярно оновлюватися й містити інформацію про напрями роботи, цільові аудиторії та регіони діяльності кожного суб'єкта. Це дасть змогу уникати дублювання проєктів, швидше знаходити партнерів для конкретних завдань і бачити, які регіони чи аудиторії залишаються неохопленими.
- Залучати організації до реалізації заходів через прозорі конкурси та пілотні проєкти в окремих регіонах. Нові підходи можна спочатку випробовувати в одному регіоні, а потім — масштабувати.
- Зберігати незалежність партнерів: довіра аудиторій до державних медійних проєктів обмежена, тож ефективніше підтримувати незалежні медіа й організації.

2.5. Забезпечити інституційну сталість урядових комунікацій

Довіра суспільства і стійкість до маніпуляцій формуються роками, тому урядові комунікації не повинні залежати від кадрових чи політичних змін. Експерти зауважували, що зараз зміна уряду часто означає зміну команд і підходів. Орієнтиром може бути естонська модель, що закріплює позапартійний характер стратегічних комунікацій і залучення до них різних секторів суспільства. Рекомендовано чітко закріпити ролі та функції органів, відповідальних за урядові та міжвідомчі комунікації, сформувати пріоритети через прозорі процедури, а також забезпечити наступність через стандарти роботи й навчальні програми для комунікаційних підрозділів.

РІВЕНЬ 3.
ОПЕРАЦІЙНІ РЕКОМЕНДАЦІЇ



Рекомендації цього рівня стосуються безпосередньо Плану заходів: як формулювати заходи, забезпечувати їх ресурсами, вимірювати результати й оновлювати План. Ці рекомендації варто врахувати вже під час розробки нового Плану.

3.1. Чітко формулювати стратегічні завдання, заходи та індикатори виконання

Рекомендовано формулювати стратегічні завдання та заходи так, щоб усі виконавці однаково розуміли, що саме і для кого потрібно зробити і якого результату досягти. Зміст кожного заходу має бути конкретним, а його зв'язок із відповідним стратегічним завданням — зрозумілим.

Індикатори виконання мають відображати не лише факт здійснення діяльності — «підготовлено матеріал», «створено механізм» чи «проведено захід» — а й очікувані якісні зміни: що поліпшилося для цільової аудиторії або в роботі відповідальних органів. Наприклад, передбачений у попередньому Плані індикатор «створено систему раннього виявлення, прогнозування та запобігання гібридним загрозам» доцільно було доповнити не лише самим фактом створення такої системи, але й показниками її практичної роботи: своєчасністю передавання попереджень відповідальним органам, їхньою придатністю для ухвалення рішень та результатами перевірки процедур реагування під час навчань.

Водночас слід визначати, за якими критеріями та за допомогою яких даних оцінюватимуть ці зміни (докладніше див. рекомендацію 3.3).

3.2. Забезпечити прозоре та деталізоване планування ресурсів для реалізації Плану заходів

Процедури підготовки урядових актів передбачають фінансове обґрунтування. Відповідно до пункту 2 § 34 Регламенту Кабінету Міністрів України, затвердженого постановою КМУ від 18 липня 2007 року №950, якщо реалізація акта потребує бюджетного фінансування, розробник проводить фінансово-економічні розрахунки, що згідно із пунктом 1.1 § 50 додаються до пояснювальної записки. Пункт 2 § 42 передбачає оприлюднення проєктів нормативно-правових актів разом із матеріалами до них для проведення публічних консультацій, якщо закон не передбачає інше. Це створює процедурну основу для відкритого обговорення ресурсного забезпечення запропонованих рішень.

Водночас пункт 3 § 34 Регламенту прямо відсилає до Методики проведення фінансово-економічних розрахунків, затвердженої наказом Мінфіну від 21 березня 2008 року №428 у редакції наказу від 6 грудня 2019 року №510, що передбачає

обґрунтування кожного заходу, фінансованого бюджетним коштом, визначення прогнозних витрат за роками та очікуваного ефекту. Цей документ вимагає також зіставляти необхідні витрати з бюджетними показниками, оцінювати додаткову потребу в коштах і визначати джерела її покриття.

Пояснювальна записка до проєкту нової Стратегії передбачає реалізацію в межах наявних видатків і визначення виконавцями обсягів і джерел фінансування конкретних заходів під час деталізованого планування. Рекомендовано узагальнити ці розрахунки відповідно до затвердженої методики у публічно доступному додатку до майбутнього Плану заходів.

Приклад прозорого оформлення — План реалізації засад медіаполітики Латвії на 2025–2027 роки. Його публічно доступний розділ V «Оцінка впливу на державний та місцеві бюджети» пов'язує заходи з бюджетними програмами, містить суми за роками та окрему графу «Необхідне додаткове фінансування». Наприклад, на підвищення медіаграмотності різних суспільних груп передбачено по €50 000 щороку за програмою Міністерства культури 27.00.00. Натомість виконання окремих заходів з удосконалення законодавства передбачене в межах наявного бюджету без визначення окремої суми. Така деталізація дозволяє публічно розмежувати заплановане фінансування та потребу в додаткових ресурсах.

Для українського Плану доцільно так само публічно відображати орієнтовні витрати за заходами й роками, відповідні бюджетні програми, погоджену підтримку в межах конкретних донорських проєктів та не профінансовані потреби. Потенційні джерела допомоги слід відокремлювати від підтвердженого фінансування. З огляду на зафіксовані у попередньому циклі випадки невиконання заходів через фінансові обмеження це допоможе завчасно визначати можливості залучення додаткових коштів або поетапного виконання завдань відповідно до їх пріоритетності. Оцінки витрат варто щорічно уточнювати з урахуванням інфляції та інших змін умов реалізації, а у звітах — зіставляти заплановані й фактичні витрати й пояснювати відхилення.

3.3. Вимірювати зміни, а не лише виконані дії

Звіти про виконання попереднього Плану переважно фіксували кількість проведених заходів. Це важлива інформація, проте вона не відповідає на головне запитання: чи стало суспільство стійкішим до інформаційних загроз? Дослідження ЦЕДЕМ пропонує доповнити звітність показниками стану інформаційного середовища: як змінюється динаміка використання різних джерел інформації, рівень довіри до медіа й офіційних джерел, поширеність фактчекінгу, вразливість до інформаційних маніпуляцій тощо. Якщо моніторити ці показники щороку за однаковою методикою, результати за різні роки можна буде порівнювати й бачити реальну динаміку. Рекомендовано на початку циклу визначити вихідні значення цих показників і очікувану динаміку.

Проводити нові дорогі дослідження для цього не обов'язково. В Україні вже є регулярні опитування, дані яких можна використовувати: щорічне дослідження «Інтерньюз-Україна» про споживання новин і довіру до медіа, індекс медіаграмотності українців від «Детектор медіа», статистика звернень до фактчекінгових ресурсів, яку запропонували використовувати експерти тощо.

Ефективність комунікацій органів влади також варто оцінювати за результатом, а не за обсягом. Експерти звертали увагу, що зараз її часто оцінюють кількістю публікацій. Кращими показниками можуть бути охоплення цільових аудиторій, довіра до офіційних джерел і зміни в поведінці чи обізнаності аудиторії.

3.4. Щорічно оцінювати ситуацію та за потреби переглядати План або Стратегію

Стратегія — довгостроковий документ, тож часто її переглядати не потрібно. Проте інформаційне середовище змінюється швидко: з'являються нові технології, платформи та способи маніпуляцій. Дослідження ЦЕДЕМ рекомендує передбачити механізм оперативного коригування цілей та заходів відповідно до істотних змін інформаційного середовища. Рекомендовано визначений порядок.

- **Щорічна оцінка ситуації.** Раз на рік аналізувати прогрес виконання Плану, динаміку ключових показників і зміни в інформаційному середовищі. Мета такої оцінки — зрозуміти, чи потребує План змін.
- **Перегляд Плану за потреби.** Якщо оцінка показує, що окремі заходи втратили актуальність або з'явилися нові виклики, План оновлюється. Це дасть змогу формалізувати адаптацію, що раніше відбувалася неформально.
- **Перегляд Стратегії лише в разі критично важливих змін.** До таких змін можна віднести припинення активних бойових дій, деокупацію значних територій, суттєві зміни в законодавстві чи технологіях. Рекомендовано заздалегідь визначити такі механізми у Стратегії, Плані чи супровідних документах.

Результати щорічної оцінки доцільно оприлюднювати й обговорювати із громадянським суспільством. Для ключових даних варто передбачити незалежну перевірку, якої не було в попередньому циклі. Це можуть робити незалежні аналітичні центри або дослідницькі установи. Звіти про виконання доцільно готувати за єдиною структурою, щоб дані за різні роки можна було порівнювати.

РІВЕНЬ 4. ПРІОРИТЕТНІ НАПРЯМИ



Рекомендації цього рівня визначають, на чому варто зосередити зусилля в наступному циклі. Вони спираються на висновки дослідження ЦЕДЕМ щодо найменш розвинених або найбільш чутливих сфер, а також на пропозиції учасників експертних обговорень. Це запобігання маніпуляціям, робота з різними аудиторіями, взаємодія із цифровими платформами, медіаграмотність, політика щодо окупованих територій і захист свободи слова.

4.1. Від реагування — до запобігання

Спростування окремих фейків залишається потрібним, але воно завжди відстає від поширення дезінформації. Експерти порівнювали протидію дезінформації із силами швидкого реагування і застерігали, що ця робота не може замінити системну та проактивну комунікацію держави з громадянами. Перехід до проактивних дій заявлений і у проєкті нової Стратегії. Рекомендовано відобразити цей перехід у Плані заходів так:

- заздалегідь пояснювати державні рішення в темах, які противник системно використовує для маніпуляцій (мобілізація, енергетика, міжнародна підтримка тощо);
- відстежувати не окремі повідомлення, а скоординовані кампанії та їхні наративи;
- розвивати навички аудиторій розпізнавати маніпуляції самостійно.

4.2. Враховувати потреби різних аудиторій

Різні групи населення отримують інформацію з різних джерел, по-різному їй довіряють і мають різний рівень навичок медіаграмотності. Тому рекомендовано:

- регулярно досліджувати цільові аудиторії та використовувати ці дані у плануванні заходів;
- визначати для заходів конкретні цільові групи, зокрема найвразливіші: людей літнього віку, жителів сільської місцевості, переселенців, жителів прифронтових і тимчасово окупованих територій, військових та їхні родини, українців за кордоном;
- добирати канали і комунікаторів, яким ці групи довіряють: місцеві медіа, лідерів громад, соцмережі та месенджери, а оскільки соцмережі — єдине джерело новин для значної частини аудиторії, тож присутність державних і достовірних незалежних джерел там має ключове значення;
- приділяти увагу регіонам, а не лише великим містам, де зосереджена більшість ініціатив.

4.3. Розвивати системну взаємодію із цифровими платформами

Цифрові платформи — соцмережі, месенджери, відеосервіси, пошукові системи, а дедалі частіше й чатботи на основі штучного інтелекту — стали головним середовищем інформаційного протистояння. Соцмережі — це водночас і ключове джерело інформації, і провідний канал поширення дезінформації. Новий виклик — спроби впливати на відповіді чатботів ШІ через масове наповнення інтернету пропагандистськими матеріалами, тобто так званий «LLM-грумінг». Дослідження ЦЕДЕМ рекомендує чітко окреслити у Плані заходи щодо взаємодії із цифровими платформами, зокрема рекомендовано:

- визначити орган, що виконуватиме функції координатора цифрових послуг відповідно до Акта про цифрові послуги (DSA) і координуватиме взаємодію із платформами;
- розробити протокол реагування і надсилання звернень щодо інформаційних інцидентів і криз з урахуванням особливостей Акта про цифрові послуги (DSA);
- поступово наближати відповідні положення національного законодавства до стандартів ЄС у контексті євроінтеграції;
- разом із громадськими організаціями та дослідниками вести діалог із платформами про ризики воєнного часу, зокрема на міжнародних майданчиках, і окремо опрацьовувати підходи до месенджерів і ШІ-сервісів.

4.4. Розвивати медіаграмотність як основу стійкості суспільства

Медіаграмотність — це здатність людини критично оцінювати інформацію, розрізняти достовірні та недостовірні джерела, розпізнавати маніпуляції. Це один із найбільш довготривалих і прозорих інструментів захисту від дезінформації, адже він не потребує обмежень свободи слова.

Індекс медіаграмотності українців помітно зріс після повномасштабного вторгнення, але останніми роками суттєво не змінився. Найвразливіші літні люди, люди із нижчим рівнем освіти, жителі сіл. Також показовий розрив між упевненістю людей у власній медіаграмотності й реальними вміннями розпізнавати дезінформацію.

Україні варто масштабувати програми медійної та інформаційної грамотності як частину загальносуспільного підходу до стійкості. Є кілька рекомендацій для цього напрямку.

- Визначити вимірювані цілі. Латвія, наприклад, поставила ціль розвинути навички медіаграмотності 75% населення до 2027 року. Україна може визначити подібні цілі, спираючись на наявний індекс медіаграмотності як сталу методику вимірювання, зокрема для найвразливіших груп.

- поширити програми на дорослих, зокрема людей літнього віку і жителів сіл, через бібліотеки, ЦНАПи, громадські центри та місцеві медіа;
- визначити координаційний механізм, оскільки у цій сфері працюють десятки організацій і проєктів;
- оцінювати ефективність заходів за зміною навичок учасників, а не лише за кількістю проведених заходів;
- підтримувати незалежні та місцеві медіа як джерела якісної інформації.

4.5. Виробити комплексну політику щодо тимчасово окупованих територій і відновлення інформаційного простору після деокупації

Попередня Стратегія визначила інформаційну реінтеграцію окремою ціллю, але саме поняття не було достатньо чітко розкрите. Експерти запропонували розрізняти щонайменше два різні завдання: комунікацію з людьми на окупованих територіях і роботу з ними після деокупації. Комунікація має враховувати відмінності між тимчасово окупованими територіями: тривалість і умови окупації, інформаційне середовище, доступні канали зв'язку та потреби місцевого населення. Це потребує диференційованих підходів до змісту повідомлень, способів їх поширення та вибору комунікаторів, яким довіряють відповідні аудиторії.

Рекомендовано дати операційне визначення інформаційної реінтеграції, планувати комунікацію з урахуванням безпеки людей на окупованих територіях і заздалегідь підготувати узгоджені відповіді на питання, які виникнуть після деокупації. Також варто забезпечити стабільне поширення українського контенту на окуповані та прифронтові території.

4.6. Захищати свободу слова та журналістів

Шкідливий контент може вводити в оману, не порушуючи закон. Без чіткого розмежування виникає ризик надмірного втручання держави у свободу слова. Рекомендовано реагувати на шкідливий контент передусім поясненням, фактчекінгом і медіаграмотністю, а обмежувальні заходи застосовувати лише тоді, коли він становить реальну загрозу національній чи інформаційній безпеці, на підставі закону і пропорційно.

Також важливо захистити журналістів і активістів від SLAPP-позовів, що мають на меті залякати їх і змусити замовкнути. Таких гарантій в Україні поки немає, але відповідний законопроєкт №16117 уже опрацьовує парламентський комітет з питань правової політики. Рекомендовано доопрацювати й ухвалити його без невиправданих зволікань.

ВИСНОВКИ

Попередній цикл реалізації Стратегії інформаційної безпеки припав на найскладніший для України період. За цей час держава, громадянське суспільство, медіа та міжнародні партнери накопичили унікальний досвід протидії інформаційній агресії. У наступному циклі Стратегії важливо врахувати цей досвід, аби він не залишився набором окремих рішень і проєктів, а став основою сталої системи.

Своєчасне ухвалення нової Стратегії інформаційної безпеки — необхідний крок для визначення спільних пріоритетів і забезпечення послідовності державної політики у цій сфері. Водночас ухвалення цього документа має супроводжуватися розробкою реалістичного Плану заходів із чітко розподіленою відповідальністю, належними ресурсами та вимірюваними результатами. Узгодження цих документів з актуалізованою Стратегією національної безпеки має забезпечити цілісність державної політики у сфері інформаційної безпеки та її відповідність загальним безпековим пріоритетам держави.

Ми закликаємо відповідальні органи актуалізувати інформаційну складову Стратегії національної безпеки, забезпечити своєчасне доопрацювання та ухвалення нової Стратегії інформаційної безпеки і Плану заходів, а також забезпечити змістовну участь організацій громадянського суспільства у цих процесах.

РЕКОМЕНДАЦІЇ

ЩОДО ПІДГОТОВКИ НОВОЇ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

та Плану заходів

HEINRICH BÖLL STIFTUNG
КИЇВ

ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА