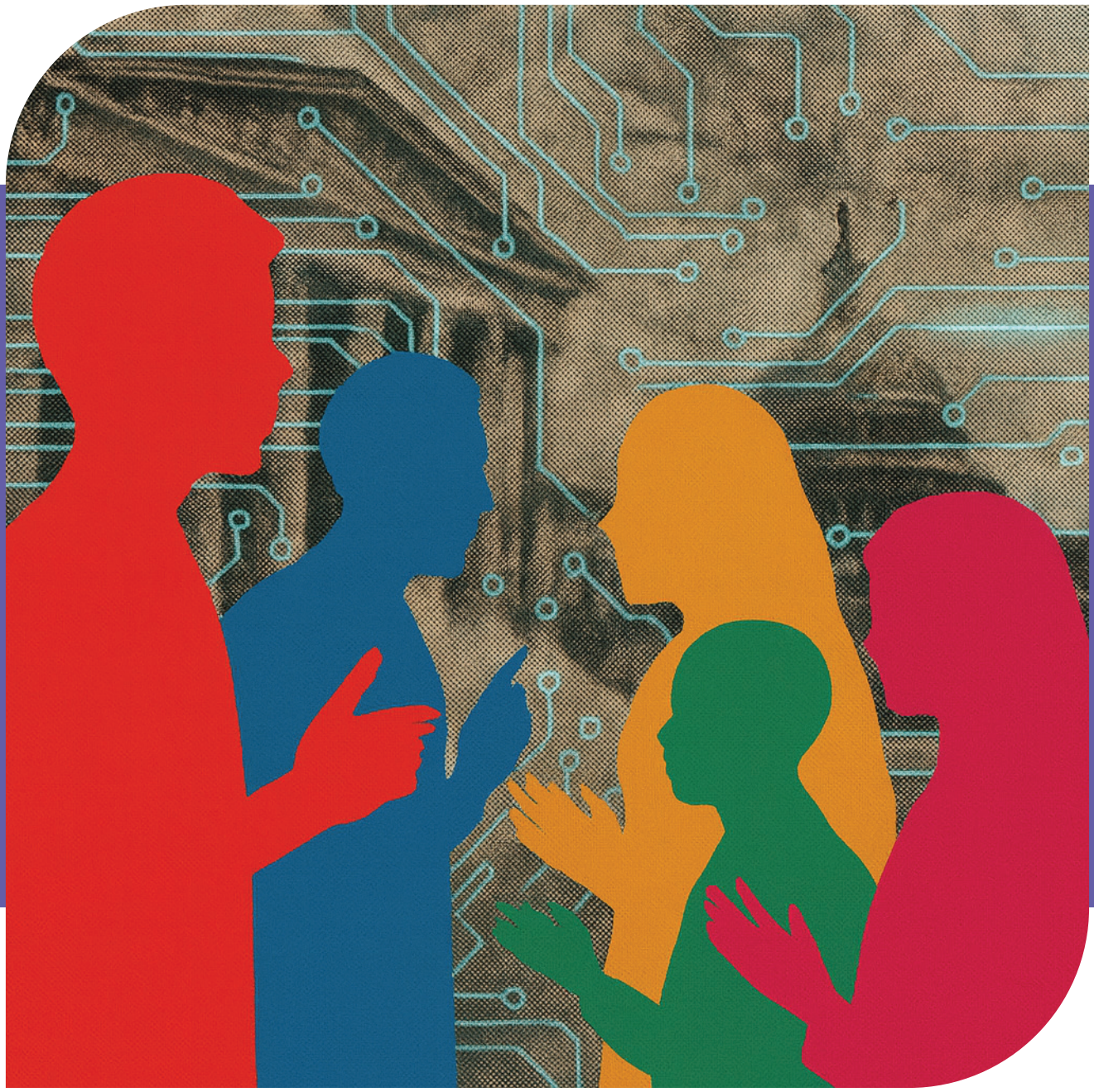
International IDEA

ПРОЄКТУВАННЯ СТІЙКОСТІ

створення інституцій для захисту інформаційних екосистем



ПРОЄКТУВАННЯ СТІЙКОСТІ

створення інституцій для захисту інформаційних екосистем

Майкл Берк

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

Публікації Міжнародного інституту демократії та сприяння виборам є політично нейтральними і не виражають конкретних національних чи політичних інтересів. Погляди, висловлені в цій публікації, не обов'язково відображають позицію Міжнародного інституту демократії та сприяння виборам або членів його Правління чи Ради. Зазначення назв країн і регіонів у цій публікації не є проявом офіційної позиції Міжнародного інституту демократії та сприяння виборам щодо правового статусу чи політики згаданих державних утворень.

Міжнародний інститут демократії та сприяння виборам (International IDEA)
Strömsborg
SE–103 34 Стокгольм
ШВЕЦІЯ
Тел.: +46 8 698 37 00
Електронна пошта: info@idea.int
Вебсайт: <https://www.idea.int>

Ілюстрація на обкладинці: Штучний інтелект, згенерований за допомогою ChatGPT
Дизайн: Міжнародний інститут демократії та сприяння виборам

DOI: <https://doi.orghttps://doi.org/10.31752/85667>

ISBN: 978-91-8137-110-9 (PDF -файл)
ISBN: 978-91-8137-111-6(друк)

Передмова

Демократичні суспільства в усьому світі стикаються з безпрецедентним тиском на свої інформаційні екосистеми. Іноземні та вітчизняні суб'єкти використовують дедалі більш складні тактики, методи і процедури для маніпулювання громадською думкою, дискредитації довіри і послаблення ключових процесів та інститутів, на яких базується демократія. Хоча вибори є вирішальним моментом як для демократії, так і для її опонентів, інформаційні загрози для демократії не обмежуються виборчим середовищем: вони постійно проникають у суспільство, знижуючи його згуртованість і стійкість. Захист демократії та її інститутів від іноземного втручання — це не лише реагування на кризи, а й активні та постійні зусилля з метою покращення інституційної стратегії та координації.

У цій публікації порушується питання інституційного дизайну та пропонуються способи, як виважений дизайн може допомогти створити стійкі інституції, що можуть забезпечувати цілісність інформації. Інституції, уповноважені розуміти та захищати національні інформаційні екосистеми, мають всі можливості для того, щоб діяти як координаційні центри демократичної стійкості в інформаційній сфері — об'єднуючи зусилля різних структур, долаючи розбіжності та забезпечуючи узгодженість, прозорість і демократичні цінності у заходах реагування. Такі інституції можуть також слугувати транскордонними сполучними ланками, сприяючи співпраці між спорідненими країнами-демократіями. Така співпраця орієнтована на створення стабільного глобального інформаційного середовища для розвитку демократії у світі.

Висновки, наведені в цій публікації, ґрунтуються на порівняльному та неупередженому аналізі підходів різних країн, при цьому визнається необхідність переймати досвід інших країн та уніфікувати міжнародні процеси. Навіть попри те, що жодна з моделей не є універсальною, публікація виявляє спільні принципи, які можуть і повинні слугувати орієнтиром для інституційного розвитку. До них належать незалежність, плюралізм, прозорість та інклюзивність.

Впроваджуючи ці принципи в інституційний дизайн від самого початку, демократичні держави можуть підсилити як легітимність, так і ефективність своїх заходів у відповідь на інформаційні загрози. Таким чином, демократичні держави не тільки посилять свою національну безпеку, але й одночасно сприятимуть формуванню довіри громадськості, захисту прав людини та забезпеченню можливості громадян робити обґрунтований вибір щодо свого майбутнього без втручання іноземних суб'єктів.

Цей документ для обговорення слугуватиме цінним джерелом інформації для розробників державної політики, практиків та організацій громадянського суспільства, які беруть участь у глобальній боротьбі за захист демократії від іноземного втручання. Завдяки обміну досвідом, узгодженню спільних демократичних принципів та інвестиціям в інституційну стійкість від етапу інституційного дизайну до реалізації на практиці, демократичні держави матимуть змогу захистити інформаційні екосистеми, якими користуються вони і ми.

Д-р Кевін Касас-Замора

Генеральний секретар Міжнародного інституту демократії та сприяння виборам (International IDEA)

зміст

СТИСЛИЙ ВИКЛАД

Інформаційні загрози, що стоять перед демократичними суспільствами та політичними процесами, особливо напередодні виборів та під час них, стають дедалі більшою проблемою для розробників державної політики і громадян в усьому світі. Маніпулятивні кампанії з боку державних і недержавних суб'єктів, що охоплюють кіберпростір, економіку, політику та інформаційну сферу, стають дедалі майстернішими. Атаки на індивідуальні та колективні процеси прийняття рішень і руйнування цілісності державних інформаційних екосистем призводять до втрати довіри суспільства і політичної поляризації. Демократичні уряди в усьому світі вжили заходів для реагування на виклики у цій сфері, зокрема створили відповідні інституції та розробили державну політику. Водночас організації громадянського суспільства також реалізували програми, покликані виявляти, запобігати та мінімізувати такі атаки на демократію. ЗМІ, експерти та інформаційно-просвітницькі програми також долучилися до боротьби з цими загрозами. З цією метою вони проводять просвітницькі кампанії задля підвищення обізнаності громадян у сфері інформаційних загроз. Це дає змогу усвідомити необхідність підвищення стійкості суспільних інститутів, насамперед у контексті прийняття рішень. Слід зазначити, що країни реагують на загрози у цій сфері по-різному, зважаючи на особливості свого контексту, правові традиції, політичні пріоритети та рівень інституційної спроможності.

Загрози інформаційній безпеці демократичних суспільств і процесів стають дедалі гострішою проблемою для розробників державної політики і громадян в усьому світі.

Незважаючи на значні зусилля, спрямовані на подолання цієї проблеми, демократичні уряди та суспільства продовжують стикатися з труднощами у виробленні та впровадженні ефективних заходів реагування на такі маніпулятивні інформаційні кампанії та операції. Розділені оперативними бар'єрами, різним рівнем розуміння або можливостей, фінансовим тиском та відсутністю політичної волі, серед інших чинників, численні внутрішні та міжнародні зацікавлені сторони дедалі частіше висловлюють нетерпіння й розчарування через відсутність відчутного прогресу. Зміна політичних пріоритетів у деяких західних країнах лише погіршила ситуацію, оскільки фінансування та

політична підтримка ініціатив уряду та громадянського суспільства, спрямованих на підвищення стійкості та розбудову потенціалу, були істотно скорочені. Однак, поряд з численними викликами, це нове середовище діяльності дає можливість переглянути підходи, що застосовувалися дотепер, та обміркувати альтернативні шляхи.

У цьому документі для обговорення аргументується, що демократичні суспільства та уряди повинні застосовувати більш скоординований, системний та організований підхід до боротьби з інформаційними загрозами. Ці загрози, що постійно еволюціонують, уражують демократії не лише під час виборчих циклів чи важливих подій у країні. Вони створюють взаємопов'язані соціальні, політичні, економічні та безпекові виклики, які не можуть бути вирішені окремим органом чи урядом, навіть якщо цей орган чи уряд має значну підтримку громадянського суспільства та інших зацікавлених сторін. Масштаб та комплексний вплив інформаційних атак поступово руйнуватимуть цілісність інформаційних екосистем у країнах, а це розхитуватиме основу демократичних процесів — право на самостійне прийняття рішень. Тому стратегія протидії наявним інформаційним загрозам та підвищення стійкості до ще невідомих або нових загроз має бути настільки ж системною. Демократичні країни мають спиратися на здобутий досвід та приклади інституцій, що вже існують у країнах, які досягли прогресу на цьому шляху, застосовуючи виважений підхід, що охоплює усе суспільство.

Підвищення внутрішньої стійкості та вдосконалення заходів реагування вимагатиме створення спеціальних механізмів для координації та впровадження цілої низки заходів на стратегічному, оперативному та політичному рівнях. Функцію координаційного центру могла б виконувати спеціальна державна установа, завданням якої було б підвищення рівня колективного усвідомлення проблем інформаційної екосистеми, налагодження системних відносин та надання рекомендацій. Така установа, створена в рамках єдиної державної системи захисту інформаційної екосистеми, могла б подолати розбіжності між оперативними повноваженнями різних органів. Як державна авторитетна організація, що є незалежною від виконавчої влади, вона також була би ідеальною платформою для мобілізації зусиль усього суспільства з метою захисту спільних демократичних цінностей і цілей. Окрім формування такої стратегії на державному рівні, ця установа також могла б сприяти координації зусиль на міжнародному рівні з іншими країнами, що дотримуються схожих поглядів, особливо з тими, які впроваджують подібні процеси. З огляду на те, що демократичні країни стикаються з подібними викликами та загрозами, їм необхідно створити нову коаліцію, яка сприятиме розвитку системного підходу до вже наявних та нових інформаційних загроз.

Цей дискусійний документ містить огляд ключових елементів, які можуть знадобитися розробникам державної політики та потенційно вітчизняним суб'єктам при обговоренні шляхів вдосконалення наявної

практики. На основі відкритих джерел, попереднього досвіду та інтерв'ю з державними службовцями, ця публікація висвітлює відповідні практики, виклики та потенційні непередбачувані наслідки. Оскільки інституційний розвиток є процесом, що значною мірою залежить від конкретного контексту, практично неможливо надати детальні рекомендації, які можна було б застосувати в усіх випадках. Цю тему можна буде продовжити в подальших дослідженнях та дискусіях. Натомість, нижче наведено ключові висновки, зроблені на основі аналізу:

1. Інформаційні загрози та ризики будуть і надалі еволюціонувати разом із технологічним поступом як частина арсеналу засобів, що використовуються ворожими силами в інформаційну епоху.

2. Кожне суспільство має унікальний соціально-політичний контекст, який визначає його підхід до інформаційних загроз. Незважаючи на спільні цінності, складно перенести успішний досвід з однієї демократичної країни в іншу, хіба що це стосується питань технічного чи процедурного характеру.

3. Суспільний підхід до протидії інформаційним загрозам повинен ґрунтуватися на всебічному розумінні державної інформаційної екосистеми, що виходить за межі традиційних ЗМІ та соціальних мереж. Цього можна досягти шляхом регулярного аналізу факторів та тенденцій, що формують інформаційну екосистему.

4. Щоб підвищити власну стійкість, держави-демократії повинні розбудовувати сучасні підходи, в основі яких лежить добре розуміння наявних загроз, проактивний підхід і цілісне бачення того, як має виглядати збалансована державна інформаційна екосистема. Таке бачення може в подальшому стати фундаментом державної стратегії, що визначатиме відповідні плани й тактики залучення зацікавлених сторін.

5. Впровадження загальносуспільного підходу до протидії інформаційним загрозам та підвищення стійкості неможливе без залучення надійних партнерів з громадянського суспільства до планування та виконання важливих функцій.

6. Необхідно створити спеціалізовану державну установу, яка буде виконувати функції координаційного центру, проводити дослідження, розбудовувати спроможності та підвищувати обізнаність, а також сприяти пошуку спільних рішень, що зміцнюють стійкість у спосіб, який є прозорим і підзвітним.

7. Дотримуючись подібного інституційного плану, демократичні країни можуть поліпшити взаємодію, ефективніше координувати свої дії та досягти більшого ефекту від вжитих заходів як у всередині країни, так і за її межами.

ВСТУП

Швидко впроваджуючи нові технології, зокрема генеративні інструменти штучного інтелекту, зловмисники збільшили швидкість і масштаби створення та поширення неправдивого або оманливого контенту.

За останні десятиліття інформаційні екосистеми різних країн стали ареною запеклої боротьби між державними та недержавними суб'єктами за увагу, політичну владу або фінансові ресурси. Зловмисні суб'єкти спрямовують вістря своєї атаки на демократичні інститути та процеси, політичних лідерів, маргіналізовані групи, маніпулюючи фактологічними даними та використовуючи різноманітні тактики викривлення інформації. Хоча під час виборчих циклів шкідлива діяльність таких суб'єктів стає більш помітною, численні факти свідчать про постійні та часто скоординовані кампанії, що охоплюють різні країни та залучають безліч іноземних і вітчизняних суб'єктів. Швидко впроваджуючи нові технології, зокрема генеративні інструменти штучного інтелекту, ворожі суб'єкти збільшили швидкість і масштаби створення та поширення неправдивого або оманливого контенту, а також зробили його більш переконливим (Chenrose і Rizzuto 2025). Поширення маніпулятивної або неправдивої інформації під час надзвичайних ситуацій, як-от пандемія Covid-19, а також під час виборчих циклів, розхитує суспільну довіру до систем управління, розпалює розбрат і розкол та підриває ініціативи в галузі охорони здоров'я (Heinmaa 2023; FIMI–ISAC 2024). Оскільки це має серйозні наслідки для внутрішньої стабільності та державного управління, багато демократичних країн почали розглядати загрозу скоординованих інформаційних кампаній з метою впливу на прийняття рішень особами та інституціями як одну з найважливіших політичних та безпекових проблем. Дедалі більше усвідомлення цих загроз свідчить про те, що культурні, мовні, соціально-політичні, геополітичні та економічні чинники лежать в основі як маніпулятивного контенту і спроб здійснення негативного впливу на прийняття індивідуальних або колективних рішень, так і заходів реагування на такі спроби з боку політичних та державних структур.

Такий розвиток ситуації спонукав багато країн вжити захисних заходів, зокрема обмежити шкідливий контент, ввести санкції проти вороже налаштованих суб'єктів, запровадити регулювання соціальних

медіаплатформ та підвищити резистентність внутрішнього середовища (Asplund і Casentini 2024; Keller, Freihse і Berger 2024; Zimonjic 2025). Громадські організації також докладають зусиль для підвищення обізнаності, поширення достовірної інформації та пригнічення джерел походження загроз. Незважаючи на ці та інші зусилля, масштаби та рівень загрози не зменшилися. Багаточисленні факти, отримані з різних джерел, спонукали до проведення кампаній з підвищення обізнаності членів суспільства. Було виявлено численні прогалини на всіх щаблях державної влади та загалом у суспільстві. Інформаційні екосистеми демократичних країн щораз частіше визнаються складними відкритими системами, які потребують всебічного управління. Такі підходи мають долати функціональну фрагментацію, покращувати координацію дій уряду, обмін інформацією та стратегічну комунікацію. Водночас вони повинні об'єднувати всіх зацікавлених суб'єктів на рівні всього суспільства, щоб ефективніше підвищувати резистентність до інформаційних загроз[1]. Зрозуміло, що це створює численні перешкоди для наявних процесів і складних інституційних відносин, що ґрунтуються на політичних компромісах і поступках, які формувалися протягом десятиліть, а то й століть. Наразі не існує готової моделі, яку можна було б легко адаптувати та впровадити.

Але це не означає, що країни з демократичним устроєм занепадають. Необхідність підтримувати відкриті та динамічні суспільства, засновані на консенсусі та збереженні індивідуальних прав і свобод, створює унікальні виклики. Ці виклики охоплюють концептуальний, стратегічний та оперативний рівні, а також фундаментальні питання управління, влади та національної ідентичності серед багатьох інших. У різних країнах досі застосовувалися підходи, що значно відрізнялися за обсягом повноважень, мірою залучення вітчизняних суб'єктів та пріоритетністю заходів. У деяких країнах основний акцент робився на прозорості та залученні громадськості за принципом «знизу догори», натомість інші країни зробили ставку на заходи протидії, спрямовані на забезпечення національної безпеки та розвідки, які не були відкритими для громадськості. Для політиків, які прагнуть розробити національні рамки та задовольнити очікування зацікавлених сторін, надзвичайно важливо розуміти ці різноманітні підходи до боротьби з маніпулюванням інформацією.

Цей документ для обговорення ґрунтується почасти на аналізові інституційних рішень, прийнятих Францією, Молдовою, Іспанією та Швецією у період з 2018 року. Аналіз був виконаний на основі загальнодоступної інформації, документів та інтерв'ю з посадовими особами. У кожному випадку шлях, обраний відповідними національними механізмами, віддзеркалює унікальний набір викликів, умов та варіантів, що стосуються їхнього контексту. До публікації увійшли кейси з практичного досвіду цих країн, враховуючи їхню

[1] Щоб ознайомитися з дефініцією та поясненням поняття «загальносуспільний підхід», зверніться до публікації EEAS (2023).

актуальність для цієї дискусії (див. блоки в розділі 3). За допомогою розгляду кейсів ілюструються різні підходи, які були реалізовані до цього часу. З огляду на постійну еволюцію цих процесів, кожен з яких характеризується особливою динамікою, проблемними питаннями, отриманим досвідом та рішеннями, важко говорити про універсальні передові практики, які можна легко перенести на терен іншої країни. Хіба що мова йде про суто технічну сторону. Водночас здобутий досвід дає змогу фахівцям-практикам зробити низку висновків, деякі з яких узагальнено в цій публікації як можливі шляхи подальшого розвитку. Зважаючи на унікальні національні обставини, розглянута тут парадигма інституційного дизайну надає можливість демократичним державам прокласти свій шлях крізь відомі суперечності політичного та організаційного характеру — наприклад, між національними та міжнародними повноваженнями, між захистом цілісності виборчого процесу та забезпеченням свободи вираження поглядів, а також між відкритою демократичною дискусією та необхідністю інтервенцій з міркувань безпеки. Якщо зосередитись на стійкості, прозорості процесів та взаємодії з ключовими спільнотами зацікавлених сторін, можна розробити більш зрілий підхід до протидії інформаційним загрозам.

Таким чином, цей документ для обговорення буде цікавий широкому колу суб'єктів, серед яких розробники державної політики, керівники інституцій, дослідники та представники громадянського суспільства з різних щаблів, включаючи урядовий, бізнесовий, академічний та громадський — всі ті, хто доклали значних зусиль і ресурсів для протидії інформаційним загрозам. Національні інформаційні екосистеми за своєю суттю є системними, тому всі рішення повинні розглядатися усіма учасниками процесу з позиції усього суспільства. Це вимагає застосування проактивного підходу до вироблення бачення стосовно того, якою має бути здорова інформаційна екосистема. Таке бачення має бути достатньо комплексним і всеохопним, щоб слугувати орієнтиром для прийняття індивідуальних рішень та сталого розвитку суспільства. Воно може бути підкріплене національною рамкою, консультаціями та законодавчими і оперативними заходами. Сподіваємося, що ця публікація сприятиме поглибленню співпраці між різними зацікавленими сторонами як на національному, так і на міжнародному рівні.

Водночас, ми вбачаємо за необхідне визначити очікування щодо того, чим ця публікація не є. З огляду на складність теми та різні вихідні позиції різних демократичних суспільств, шлях до спільного майбутнього не буде однаковим для усіх країн. Тому в цій роботі ми уникаємо настановчого прескриптивного підходу. Натомість у кожній частині розділу 3 ми порушуємо питання, які спонукають до пошуку конкретних рішень, що можуть відповідати або не відповідати нормативним та соціально-політичним умовам демократичного суспільства. Оскільки демократії стикаються з подібними загрозами та викликами, вони можуть здійснювати процеси розбудови національних інституцій, одночасно обмінюючись інформацією та координуючи свої дії між собою. Блок, що окреслює теорію змін для демократичних країн,

допомагає виробити краще розуміння того, як можна гармонізувати зусилля з координації на національному та міжнародному рівнях, підсилюючи їхній ефект. Демократичні країни мають змогу обрати такі внутрішні процеси, які сприятимуть досягненню суспільного блага. Цей документ для обговорення має на меті запропонувати загальні обриси того, як цього можна досягти.

Розділ 1

ПЕРЕДУМОВИ: ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА ПОВ'ЯЗАНІ З НИМИ ВИКЛИКИ

Глобальне інформаційне середовище, що характеризується високим рівнем взаємопов'язаності, об'єднує людей і суспільства через кордони. Це не тільки відкриває нові можливості та дає можливість здобути нові знання, але й створює нові ризики та загрози. В останні десятиліття все більше уваги приділяється ролі інформації, її створенню, поширенню та особливо впливу на прийняття рішень у політичній, економічній та соціальній сферах. Здатність людей ухвалювати обґрунтовані, самостійно прийняті рішення щодо свого майбутнього традиційно вважається основою демократії.

Права людини передбачають наявність умов, що дають змогу їх реалізувати. До таких умов належать доступ до достовірної інформації, вільні ЗМІ, прозорі джерела, цифрова грамотність та здатність робити незалежний вибір, зокрема через обраних представників. Те, як ці умови формуються в кожному національному контексті, залежить від його правил, норм та інституцій, а також від обізнаності громадян та їхнього розуміння спільної реальності. Саме це спільне сприйняття реальності в кінцевому підсумку формує індивідуальний вибір, а отже, і державну політику, правила, норми та очікування. Ці та багато інших чинників безпосередньо впливають на процвітання, стабільність і, за необхідності, виживання суспільства. Створена завдяки складній, а нині технологічно підкріпленій мережі інформатизованих процесів та взаємовідносин між родинами, громадами та організаціями, ця реальність виявляється у вигляді надзвичайно динамічної та адаптивної національної інформаційної екосистеми.

У демократичних суспільствах інформаційні екосистеми є здебільшого спільними відкритими просторами, які постійно еволюціонують під впливом вхідних даних (наприклад, публікацій у соціальних мережах, маркетингу, новин, політичної реклами, чуток та неправдивої інформації), які вводять у суспільний дискурс різні суб'єкти, серед яких — закордонні вороги та опоненти, а також умов, що впливають на їхню поведінку

та динаміку (наприклад, нормативно-правові акти, інфраструктура, власність, суспільні норми). Хоча інформаційні екосистеми існували як мережі обміну інформацією з самого початку існування людства, з появою Інтернету їхня складність та динамічність значно зросли. Мінливі умови та нерівномірний доступ до інформації на різних рівнях прийняття рішень чинять значний тиск на осіб та організації, які намагаються зрозуміти реальність. Структурування та керування інформаційними потоками задля суспільно значущих цілей стає дедалі складнішим завданням, особливо на тлі вимоги сьогодення забезпечити широкий демократичний консенсус. Коли погіршення якості інформації або неспроможність досягти бажаних результатів починають руйнувати цю складну екосистему, здатність суспільства гарантувати її безперервність значно зменшується (OECD 2024a).

Впродовж останніх років якість цих вхідних даних та умов, а також довіра між найважливішими вузлами соціальних мереж дедалі більше зазнають атак з боку іноземних та вітчизняних суб'єктів. Гібридні операції іноземних державних суб'єктів[2], дезінформаційні кампанії екстремістських або радикальних угруповань, атаки на критичну інформаційну інфраструктуру та онлайн-шахрайство, серед іншого, загрожують національним інтересам та соціальній стабільності (VIGINUM 2025; Sicurella and Morača 2025). Ці операції відбуваються на різних рівнях — когнітивному, психологічному, технологічному, фізичному — і по-різному впливають на нашу індивідуальну та колективну реальність і процеси прийняття рішень. Такі дії з поширення маніпулятивного контенту, що мають транскордонний і дедалі масштабніший характер, розхитують довіру громадськості до інституцій, процедур та системи управління загалом. Громадяни багатьох демократичних країн і без того стикаються з необхідністю робити складний вибір щодо соціально-економічних питань, а поширення неправдивої інформації може ще більше послабити їхню здатність приймати самостійні та обґрунтовані рішення. Крім того, ці дії часто мають на меті послабити соціальну згуртованість та здатність впроваджувати ефективну політику. З часу президентських виборів у США 2016 року накопичилася значна кількість доказів, які свідчать про те, що іноземні суб'єкти та їхні представники втручаються у вибори або інші суспільно-значущі події, використовуючи системні та інституційні вразливості держав (EEAS 2025; McPherson 2025). Наприклад, російські інформаційні операції виходять за межі конкретної країни і відбуваються на постійній основі, особливо в країнах, які Росія вважає стратегічно важливими (Châtelet and Lesplingart 2025). Інші держави, як-от Китай та Іран, також активізували свої кампанії з дезінформації та маніпулювання громадською думкою в останні роки (Charon and Jeangène Vilmer 2021; ODNI, FBI and CISA 2024). Зловмисники, від держав до екстремістських суспільних рухів та корпорацій, використовують різноманітні цифрові технології та методи для впливу на результати виборів, просування вигідного їм суспільного

Ці заходи часто мають на меті послабити соціальну згуртованість та спроможність реалізовувати ефективну політику.

[2] Для отримання додаткової інформації стосовно гібридних загроз див. Hybrid CoE (без дати).

порядку денного або маніпулювання сприйняттям громадянами питань внутрішньої та зовнішньої політики (Wanless and Berk 2019; Bicu n.d.).

Попри дедалі більшого усвідомлення цих загроз у демократичних суспільствах, різні люди можуть сприймати їх по-різному. Багато чинників, як-от культурні та політичні норми, соціальна структура і згуртованість, рівень освіти, а також такі умови, як географічне розташування, військова міць і соціально-економічний розвиток, впливають на те, як суспільства інтерпретують ці загрози та їхній можливий вплив. Різна вага цих чинників у кожному конкретному контексті, своєю чергою, безпосередньо впливає на те, як громадяни, організації громадянського суспільства та особи, що приймають рішення, формулюють національний дискурс і розробляють можливі заходи реагування. Крім того, навіть у юрисдикціях, де суспільство має підвищену обізнаність про інформаційні загрози, заходи реагування на сьогоднішній день різняться за обсягом і спрямованістю. Безумовно, рішення щодо можливих дій залежать від тієї оптики, крізь яку особи, що приймають рішення, розглядають суспільні питання та оцінюють ризики. Наприклад, реагування держав на іноземне втручання може відрізнятися залежно від його наслідків (наприклад, економічний тиск, корупція, фальсифікація фактів та істини або шпигунство), залучених суб'єктів (наприклад, іноземні держави, посередники, злочинні угруповання), змісту (наприклад, неправдиві повідомлення, дезінформація) та пов'язаних з цим дій.

Таким чином, за відсутності обов'язкових міжнародних законів або загальноприйнятих норм, що визначають відповідальну поведінку в інформаційному середовищі (поза кіберпростором), різні країни по-різному трактують ці загрози та реагують на них. Це призводить до виникнення повноважень та механізмів, які зазвичай зосереджуються на вузькому колі злочинних суб'єктів, факторів або умов, що стоять за цією загрозою. У багатьох демократичних країнах цей процес включає моніторинг відкритих джерел, обмін інформацією та координацію між органами безпеки та розвідки, з різним ступенем залучення громадянського суспільства, експертів та ЗМІ. У міру постійної еволюції інформаційних загроз та національних екосистем, внесення нових механізмів ускладнює координацію та потребує залучення нових ресурсів.

Це, своєю чергою, створює дві важливі взаємопов'язані дилеми в демократичних країнах. По-перше, сек'юритизація питань, що стосуються національної інформаційної екосистеми, — що є виправданим, особливо у випадках, в яких фігурують іноземні суб'єкти, — посилює безпековий апарат, одночасно звужуючи співпрацю з громадським сектором. Водночас це перешкоджає згуртованій відповіді усього суспільства та знижує його резистентність, адже обидві ці складові базуються на залученні громадян. Це особливо очевидно в поляризованих суспільствах, де рівень довіри до державних інституцій та ЗМІ є нижчим. Можливий перехід до авторитарних заходів за певних

обставин становить реальну небезпеку для цінностей демократії. По-друге, розгляд викликів інформаційної екосистеми переважно крізь призму загроз обмежує спектр можливих рішень, не пов'язаних із безпекою, щодо системних вразливостей та ризиків, що впливають на все суспільство. Зміцнення мультикультурних зв'язків між громадянами, поліпшення можливостей працевлаштування молоді та розробка національних проєктів, які також сприяють формуванню толерантності, взаєморозуміння та духу співпраці серед населення, з більшою ймовірністю призведуть до посилення стійкості до іноземного втручання. На доповнення до цих внутрішніх викликів і попри поточні міжнародні координаційні зусилля, демократичні країни значною мірою відрізняються за ступенем визнання наявних бар'єрів і прогалин. Це, своєю чергою, впливає на визначення пріоритетності ресурсів і здатність країн протидіяти різним формам маніпулювання інформацією та втручання (наприклад, країни Глобального Півдня зазнали труднощів із підтримкою спротиву України російському вторгненню).

Щоб протистояти цим взаємопов'язаним соціальним, політичним, економічним та безпековим викликам, демократичні суспільства мають розробити більш виважений підхід до інформаційних загроз та ризиків. Це вже було визнано в кількох нещодавніх закликах до дії з боку міжнародних організацій та демократичних урядів (ОЕСР 2022; Уряд Канади, Уряд США та Уряд Великої Британії 2024). В основі такого підходу, що ґрунтується на комплексному розумінні того, що становить національну інформаційну екосистему, має міститись перспективне бачення, яке привертає увагу та мобілізує зацікавлені сторони, наприклад, шляхом розробки та впровадження концепції цифрового громадянства (Council of Europe n.d.; OECD n.d.b; United States Department of State n.d.). Для того, щоб громадяни могли досягати своїх цілей у безпечному та захищеному демократичному середовищі, також необхідна відповідна інституційна інфраструктура, яка здатна реагувати на конкретні інциденти та сприяти формуванню умов, що підтримують здоровішу внутрішню інформаційну екосистему.

Розділ 2

ЧОМУ У ДЕМОКРАТИЧНИХ КРАЇНАХ ПОТРІБНІ СПЕЦІАЛІЗОВАНІ ІНСТИТУЦІЇ ДЛЯ ВИРІШЕННЯ ПРОБЛЕМ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Спеціалізовані інституції необхідні для сприяння ухваленню колективних рішень, забезпечення дотримання правил та інформування про очікувані норми поведінки.

Інституції покликані відігравати важливу роль у демократичних державах на різних рівнях. Зі стратегічної точки зору, вони забезпечують прогнозоване функціонування політичної системи шляхом розширення повноважень та обмеження влади уряду, захисту прав громадян та сприяння здоровій демократичній культурі. З оперативної точки зору, вони досягають цих цілей різними засобами, зокрема шляхом управління та передачі відповідної інформації за допомогою визначених протоколів та процедур, що забезпечують безперервність функціонування системи. У соціальному та політичному плані інституції необхідні для сприяння колективним рішенням, дотримання правил та інформування про очікувані норми поведінки. Наприклад, більшість демократичних держав мають виборчі комісії та допоміжні державні органи, які контролюють процеси голосування та забезпечують дотримання правових норм щодо тактики передвиборчої кампанії, фінансування передвиборчої кампанії та справедливого доступу до засобів масової інформації. Інші державні інституції захищають громадянські та політичні права, необхідні для політичної участі, зокрема свободу вираження поглядів та об'єднання.

З огляду на численні системні виклики в інформаційній сфері, різні демократичні країни за останні роки розробили низку заходів реагування, що враховують різноманітні контексти, правові традиції, політичні пріоритети та рівень інституційної спроможності. Деякі країни створили спеціальні агентства для протидії дезінформації та зловмисному впливу з-за кордону, водночас інші держави доручили ці функції вже наявним виборчим комісіям, міністерствам закордонних справ або органам національної безпеки. Багато країн створили механізми для вивчення або просування міжінституційних заходів у різних формах. Додаткові ініціативи в галузі регулювання ЗМІ та громадянського суспільства

також сприяли підвищенню обізнаності суспільства про загрози та їхній можливий вплив на суспільство (Sessa et al. 2024)[3].

Проте, незважаючи на ці численні та різноманітні зусилля, демократичні країни продовжують стикатися з політичними та безпековими ризиками, що постають у результаті скоординованих кампаній зловмисних суб'єктів. Рівень обізнаності не є однаковим серед різних груп інтересів, а регулювання контенту та заклики до відстоювання «правди» мають зворотний ефект через звинувачення урядів у стеженні або порушенні основних свобод. Довгостроковий вплив на суспільство інших зусиль, зокрема перевірки фактів, попередження або протидія зловмисним кампаніям шляхом поліпшення стратегічних комунікацій, також залишається неясним за межами експериментів та окремих випадків. Як зазначають деякі експерти, хоча дотепер було здійснено чимало спроб протидії дезінформації, у порівнянні з надзвичайною різноманітністю і масштабним характером інформаційних загроз усі ці спроби можна алегорично порівняти з грою «вдар крота» (Bradshaw 2020; Johnson 2024). Це не означає, що зусилля протидії дезінформації є марними. Демократичні країни досягли значних успіхів у розумінні інформаційних загроз та визнанні необхідності їх усунення як найвищого пріоритету. Надалі важливо, щоб вони провели відвертий аналіз отриманого досвіду та перетворили знання, отримані в результаті цього досвіду, на новий, більш зрілий підхід до захисту національних інформаційних екосистем та протидії новим загрозам. Щоб досягнути поставленої мети, демократичним країнам потрібна нова система, яка б організовувала та спрямовувала розрізнені зусилля з більшою узгодженістю.

Демократичні країни досягли значних успіхів у розумінні інформаційних загроз та визнанні необхідності їх усунення як найважливішого пріоритету.

У суспільних системах інформаційні атаки спрямовані на використання психологічних та когнітивних вразливостей у тому, як люди сприймають, тлумачать та реагують на інформацію (Giannopoulos, Smith and Theocharidou 2021; NATO 2025). Ці атаки, вістря яких спрямовані на точкові ситуації або моделі поведінки, мають на меті зруйнувати певні суспільні відносини, що певною мірою забезпечують соціально-політичну та економічну стабільність. Це питання стає особливо гострим під час криз та конфліктів. Саме тому суспільна стійкість до інформаційних загроз є настільки важливою. На суспільному рівні стійкість вимагає згуртованості між членами суспільства, що проявляється у почутті приналежності до спільноти, ідентичності, співпричетності та взаємній довірі. Саме такий клімат у середовищі стимулює співпрацю та конструктивні дії, особливо в стресових ситуаціях.

Аби забезпечити стійкість демократичних суспільств, необхідні спеціальні механізми для координації та підтримки різних заходів на стратегічному, оперативному та політичному рівнях. Одним із можливих таких кроків може бути створення спеціалізованої державної установи, яка буде займатися підвищенням обізнаності громадян стосовно

[3] Для отримання додаткової інформації стосовно офіційних підходів див. також **European Commission** (без дати) та **OECD** (без дати).

проблем і вразливостей інформаційної екосистеми, сприятиме у налагодженні системних відносин між різними суб'єктами і надаватиме рекомендації для розробників державної політики і фахівців-практиків. Ця державна установа, створена в рамках єдиної державної політики щодо захисту цілісності та безпеки інформаційної екосистеми, буде заповнювати прогалини в оперативних повноваженнях та мобілізувати зусилля всього суспільства на підтримку спільних демократичних цінностей і завдань[4].

Окрім виконання таких важливих функцій, як інформаційно-просвітницькі зусилля і координація дій, ця установа відіграватиме ключову роль у виявленні та заохоченні процесів, які сприяють формуванню здорової національної інформаційної екосистеми як суспільного блага. Це відбувається завдяки тому, що фізичні та юридичні особи послідовно формують власну ідентичність та моделі поведінки у межах інформаційної екосистеми. Така спеціалізована установа за належних умов і в межах відповідної структури може стати надійним і відповідальним органом, що консолідує різні суспільні групи, діє в інтересах та на благо суспільства. Цього можна досягти шляхом досліджень, аналізу і збору свідчень, а також завдяки залученню широкого кола експертів на засадах прозорості та співпраці. Використовуючи такий підхід, демократичні держави можуть як інституціоналізувати, так і кодифікувати відповідні процеси і моделі поведінки, водночас розробляючи заходи захисту від партійного ідеологічного втручання та створюючи процедурні бар'єри проти авторитаризму.

[4] Цей процес багато в чому нагадуватиме еволюцію національних підходів до загроз кібербезпеці. Див. збірку відповідних документів у Центрі передового досвіду НАТО з питань кіберзахисту.

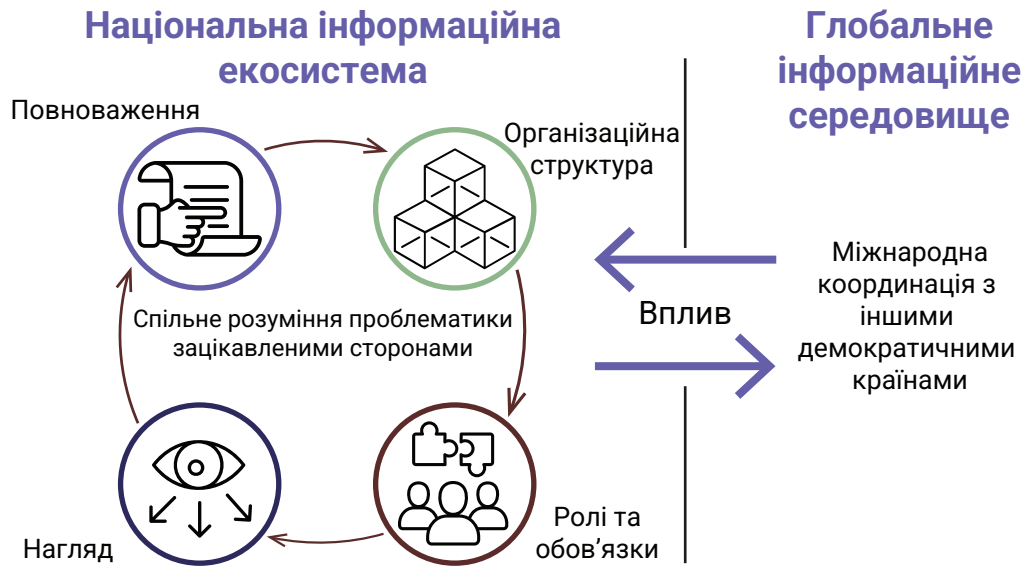
Розділ 3

КЛЮЧОВІ ЕЛЕМЕНТИ ІНСТИТУЦІЙНОГО ДИЗАЙНУ

У цьому розділі викладено основні елементи інституційного дизайну, які повинні брати до уваги розробники державної політики, плануючи заходи реагування на інформаційні загрози. Ці складові інституційного дизайну були виявлені на основі вивчення практичного досвіду та проведення інтерв'ю з державними службовцями, які керували подібними заходами у своїх країнах. Він також містить чотири кейси з досвіду Швеції, Іспанії, Франції та Молдови. Уряди цих країн були новаторами у процесі інституційної розбудови в останні роки. Подібні ініціативи продовжують розвиватися, як долаючи певні обмеження, так і відкриваючи нові можливості. Включення кейсів з практичного досвіду декількох країн до цього документа не варто тлумачити як їхнє беззаперечне схвалення чи взірець для наслідування, а лише як ілюстрацію. Інституційний розвиток — це процес, який значною мірою залежить від контексту та є політично чутливим, тому важко екстраполювати, чи те, що працює «тут», буде працювати «там». Ось чому, якщо юрисдикція бажатиме скопіювати кращі практики з досвіду іншої країни, апробовані та перевірені, це може дати незадовільний або відмінний від очікуваного результат, хіба що йдеться про винятково технічні або процедурні питання. Ось чому цей документ присвячений обговоренню загальних положень, які дадуть змогу демократичним країнам спершу візуалізувати спільний шлях. Пізніше, за необхідності, цей документ, у якому презентується візія і рамкова модель, може бути доповнений практичними прикладами з досвіду різних юрисдикцій, в яких розкриваються індивідуальні особливості застосування різних методів і процесів. Переваги вироблення спільної візії полягають у тому, що це дає змогу демократичним суспільствам проводити більш відкриті дискусії стосовно спільних викликів, питань і дилем, які необхідно вирішити, перш ніж формувати національний, адаптований до місцевого контексту підхід разом з обсягом повноважень відповідних органів. Незважаючи на те, що різні країни можуть мати різні погляди на загрози в інформаційному середовищі або особливості інформаційної екосистеми, вони, імовірно, будуть здатні досягнути істотного прогресу на шляху до ліпшої

координації та співпраці, якщо в основі такої співпраці лежатиме візія, спільно прийнята і осмислена ними. Це може слугувати дороговказом для юрисдикцій у міру того, як вони гармонізують процеси і підходи всередині кожної країни, з плином часу удосконалюючи спроможності та ресурсний потенціал (див. Рисунок 3.1).

Рисунок 3.1. **Елементи інституційного дизайну**



Примітка: Створено з використанням піктограм з Noun Project, авторами яких є Кей Креатів, Тіні Суміарсіх і Фебрі Ардіанто (Keyy Creative, Tini Sumiarsih, Febri Ardianto).
Джерело: Створено автором цієї публікації.

3.1. СПІЛЬНЕ УСВІДОМЛЕННЯ ТА РОЗУМІННЯ

Перш ніж обговорювати ключові елементи інституційного дизайну, важливо розглянути фундаментальне питання, що визначає стійкість суспільства до загроз. В усіх новітніх підходах, розглянутих у цій публікації, наявність «спільного усвідомлення» була виділена як ключовий фундаментальний елемент, а його відсутність — як найважливіша перешкода. Незважаючи на те, які структури були впроваджені в різних країнах та якими повноваженнями вони наділені на сьогодні, усі юрисдикції стикалися з цілою низкою проблемних питань на оперативному, організаційному та стратегічному рівні. Дуже часто ці проблеми поставали через різний рівень усвідомлення та розуміння загроз, неоднакове тлумачення термінів, особливості впровадження загальнодержавної політики або інші відмінності, що зумовлюють неоднаковий вибір можливих варіантів. Складно буде створити злагоджену національну структуру та виробити єдиний підхід, якщо представники різних щаблів державної влади, громадянського

суспільства, академічної спільноти та бізнесу продовжуватимуть діяти на різних діапазонах.

Наразі підвищення обізнаності щодо інформаційних загроз розуміється насамперед як підвищення рівня усвідомлення громадськістю кампаній з дезінформації, фейкових новин, кіберфішингу, а також можливих запобіжних заходів. Ці заходи включають стратегічні комунікаційні кампанії, що організовані переважно за принципом «зверху донизу», програми цифрової грамотності або інформаційні матеріали у ЗМІ. Подібні інформаційно-просвітницькі кампанії мають на меті привернути увагу громадян до небезпечних явищ, як-от маніпулювання громадською думкою, та можливих заходів протидії.

Інформаційно-просвітницькі кампанії можуть дати бажані результати, як-от зміна когнітивних та поведінкових шаблонів, за умови, що громадяни матимуть доступ до такої інформації. Успіх інформаційно-просвітницьких кампаній також залежить від індивідуальної здатності людей сприймати головні меседжі. Хоча вплив цих методів залишається предметом дискусій, слід визнати, що, незважаючи на численні зусилля, сприйняття інформаційних загроз всередині демократичних суспільств істотно різниться. Безумовно, це стосується всіх зацікавлених сторін, включаючи державні установи, де досить вузько визначені повноваження впливають на те, як особи, що ухвалюють рішення, розуміють своє оперативне середовище та наявні варіанти дій. Якщо інформаційна екосистема є надмірно поляризована, а при цьому у суспільстві спостерігається низький рівень довіри до інструментів управління, через нерівномірне сприйняття загроз та їхніх наслідків можуть виникати серйозні політичні та стратегічні виклики.

Демократії повинні не обмежуватися таким підходом, в основі якого лежить розуміння загроз і способів реагування на них. Натомість, суспільства повинні формувати більш широке уявлення про те, що означає проактивно будувати та захищати свої інформаційні екосистеми, наприклад, як захистити інформацію на загальнодержавному рівні. Такі концепції мають бути достатньо широкими, щоб їх можна було використовувати як основу для розробки стратегій у багатьох сферах, а також щоб вони були привабливими для різних поколінь і могли стати основою для нового соціально-політичного та культурного дискурсу. Переступаючи межі вузьких політичних завдань або програм, такі концепції мають більше шансів залучити все суспільство до співпраці та сприяти зміцненню його стійкості в довгостроковій перспективі (Комітет Ради Європи з політичних питань та демократії 2025).

Демократичні країни повинні виробити чітке розуміння того, як активно будувати та захищати свої інформаційні екосистеми.

Вироблення такого розуміння дасть змогу демократичним державам досягти двох однаково важливих результатів: по-перше, визначити довгострокові стратегічні цілі національного розвитку, за якими кожен зможе оцінювати власні успіхи; по-друге, скоригувати поточні зусилля із розроблення державної політики та оперативні заходи реагування, а це дасть змогу подолати розрив між сьогоденням і майбутнім. Першим

кроком у цьому напрямку має стати формування єдиного позитивного бачення того, якою має бути надійна інформаційна екосистема, побудована на демократичних цінностях і принципах. У результаті цього зацікавлені сторони не лише зможуть визначити спільні амбітні цілі, а й сформувати уявлення про те, яких умов вони прагнуть досягнути у соціальній, економічній, культурній сфері, розробляючи і впроваджуючи державну політику та забезпечуючи цільове фінансування. У разі проведення національних публічних консультацій з цих питань, якщо вони будуть прозорими та відвертими, це допоможе сформувати єдине бачення побудови майбутнього, а також розглянути питання національної та культурної ідентичності, процвітання, безпеки, верховенства права, справедливості та свободи. Крім того, це може стати джерелом натхнення та стимулом до дій, що зміцнить почуття приналежності та сприятиме формуванню спільноти.

Ця дискусія повинна охоплювати питання, що стосуються системної ролі здорової інформаційної екосистеми, шляхів її створення, а також уразливих місць і загроз. Усі національні суб'єкти можуть скористатися результатами цього процесу для досягнення багатьох конкретних цілей, від укорінення загальноприйнятих норм поведінки до визначення параметрів політично обґрунтованої державної політики та регуляторних механізмів і безлічі інших завдань[5].

Справді, в певних умовах може бути неможливо йти цим шляхом через високий рівень поляризації суспільства, низький рівень довіри до ЗМІ та уряду або інші обставини, зокрема, відкриті конфлікти. У таких випадках лідери можуть відчувати тиск і тому обирати вигідний для себе варіант, реагуючи на інформаційні загрози за допомогою таких механізмів як законодавчі акти, виконавчі розпорядження або стратегічна комунікація. Проте в демократичному суспільстві такий підхід у довгостроковій перспективі несе значні ризики. Щонайменше він повинен супроводжуватися чіткою та прозорою комунікацією щодо цілей та термінів. Варто пам'ятати, що атаки на достовірність інформації часто скеровані проти тих самих засобів масової інформації, неурядових організацій (НУО) та процедур, які становлять основу демократичної стійкості та верховенства права. Оскільки ці організації безпосередньо відчувають негативні наслідки кампаній впливу, вони не тільки більш чутливі до загроз, але й можуть стати найбільш потужними партнерами у захисті від них.

За будь-яких обставин зрілий підхід, що визнає цілісний вплив інформаційних екосистем на суспільство в цілому, повинен також передбачати розробку практичних заходів, що підвищують як резистентність, так і ефективність формування державної політики. Багато в чому національна інформаційна екосистема має сприйматися як нова критична інфраструктура, на якій базується сталий розвиток сучасних суспільств. Безперечно, формування резистентності

[5] Щоб отримати додаткову інформацію та ознайомитися з ідеями, які надихають, див. AP4D (2024).

суспільства, здатного витримувати інформаційні потрясіння та швидко відновлюватися після них, — це не просте завдання на кшталт спорудження будівлі із цегли. Це складний суспільно-політичний процес, який починається з того, що всі зацікавлені сторони набувають спільних знань про те, як закони, нормативні акти та впроваджені ними політичні заходи впливатимуть на національну інформаційну екосистему з часом. По суті, жодна система не може існувати або відновлюватися без розуміння своїх критично важливих характеристик. А це розуміння може з'явитися лише завдяки організованим і скоординованим зусиллям з метою аналізу соціально-політичних, економічних та інших відповідних чинників, які впливають на те, як національні інформаційні екосистеми розвиваються з часом (Wanless, Lai and Hicks 2025).
Якщо серед лідерів думок і керівників буде сформовано таке науково обґрунтоване спільне розуміння, це, безумовно, допоможе подолати ті бар'єри, з якими стикаються особи, що розробляють та втілюють у життя державну політику. Важливо також додати, що цей аналіз, підкріплений доказовими даними, може також вплинути на процес формування національної ідентичності та індивідуального самоусвідомлення. Окрім того, це впливає на готовність громадян захищати свої суспільства, а також дбати про їхній розвиток відповідно до демократичних принципів. Активна участь членів громадянського суспільства в консультативних процесах допоможе посилити систему стримувань і противаг, підвищити підзвітність і прозорість, а також довіру до демократичних процесів та інститутів. Усі ці ефекти сприятимуть зміцненню стійкості суспільства (OECD 2020).

Розбудова резистентності суспільства, здатного витримувати інформаційні шоки та швидко відновлюватися після них, — це не просте завдання на кшталт спорудження будівлі із цегли і бетону.

Питання для розмірковування, що стосуються спільного усвідомлення та розуміння:

- Які ключові суб'єкти на національному рівні визначають інформаційну екосистему та яку роль вони відіграють? До таких суб'єктів можуть належати департаменти, асоціації, засоби масової інформації, галузеві гравці, групи інтересів.
- Як спеціалізована установа із захисту доброчесності інформації може забезпечити однакове розуміння понять і термінів різними суб'єктами таким чином, щоб допомогти кожному з них визначити свою роль та обов'язки в національній інформаційній екосистемі?
- Які механізми та підходи можуть допомогти сформувати єдине уявлення про тенденції в національній інформаційній екосистемі, включаючи загрози, ризики та вразливі місця? Яку роль повинна відігравати спеціалізована установа в плануванні сценаріїв або системах раннього попередження?
- Які види інформації, доказів, оперативно-аналітичних або розвідувальних даних чи експертних знань слід вважати найбільш важливими для формування єдиного бачення?

Блок 3.1. **Шведське агентство психологічного захисту**

Державне агентство з питань психологічного захисту Швеції (Myndigheten för psykologiskt försvar, SPDA) оберігає відкрите і демократичне суспільство Швеції та вільне формування думки шляхом виявлення, аналізу та протидії шкідливому впливу з-за кордону, дезінформації та іншим видам оманливої інформації, що спрямовані проти Швеції та її національних інтересів (SPDA n.d.).

Заснована Міністерством оборони в січні 2022 року, ця урядова установа має своїм головним завданням координацію та розвиток психологічного захисту Швеції у співпраці з державними органами та іншими суспільними суб'єктами. Визнаючи важливість загальносуспільного підходу до формування стійкості та оборони, агентство надає підтримку урядовим установам, муніципалітетам, регіонам, зацікавленим сторонам зі сфери бізнесу та іншим організаціям у Швеції у зміцненні спроможності населення протистояти інформаційним загрозам та реагувати на них. Цей підхід був розроблений у партнерстві з кількома установами на основі багаторічного досвіду зміцнення психологічного захисту, набутого під час холодної війни.

Шведське агентство психологічного захисту працює над підвищенням обізнаності суспільства, налагодженням спільної робочої мови та впровадженням спільних практик за допомогою досліджень, посібників, навчальних курсів, співпраці з громадянським суспільством, навчальних фільмів та підвищення медіаграмотності. Ці зусилля спрямовані на мотивування всіх зацікавлених сторін до підвищення готовності шведського суспільства до будь-яких загроз або криз. Агентство також співпрацює з міжнародними партнерами з метою обміну інформацією про загрози та аналізу досягнень і успішних практик (Tofvesson і Kozłowski 2024).

3.2. **МАНДАТ**

Визначення сфери діяльності та повноважень інституції, яка має на меті як захист національної інформаційної екосистеми, так і сприяння її розвитку відповідно до демократичних цінностей, — це критично важливе політичне рішення. Який орган надає такі повноваження і з якою метою? Які пріоритети та обов'язки до них належатимуть? Чи буде потреба прийняти нове законодавство? Як забезпечити, щоб ці повноваження залишалися актуальними в умовах мінливої реальності?

Залежно від культурних, соціальних та політичних обставин, відповіді на ці та пов'язані з ними питання будуть відрізнятися в різних демократичних країнах. Наразі, незважаючи на кілька прикладів, із яких можна почерпнути корисний досвід, не існує універсальної моделі, яку можна було б легко перенести в інші країни. Водночас існують спільні принципи, як-от бажання захищати демократичні права і свободи, сильний громадський контроль, прозорість і підзвітність, незалежність від виконавчої влади та підхід, що охоплює все суспільство, які створюють міцну основу для підвищення довіри громадян до демократичного врядування та сприяння міжнародній співпраці та координації.

У більшості випадків національні інституції або ініціативи з'явилися завдяки рішенням центрального уряду країни. Визнаючи нові та мінливі інформаційні загрози, ці уряди почали створювати ресурси для моніторингу та координації відповідних заходів на рівні усього апарату

влади. Ці ініціативи, що мають винятково оперативний характер, насамперед орієнтовані на виявлення конкретних загроз, а також на удосконалення координації з іншими учасниками процесу для мінімізації їхнього впливу.

Спираючись на інтерв'ю, проведені для цієї публікації, а також на попередній досвід у цій галузі, можна зробити висновок, що наразі перед більшістю демократичних урядів постали дві основні проблеми. По-перше, державні органи не обмінюються між собою інформацією та аналітичними даними у повному обсязі. На заваді комплексним діям уряду часто стає вузькоспрямоване законодавство, а також неоднаковий рівень повноважень і компетентності. У зв'язку з цим найкращим підходом на сьогодні є координація міжвідомчих робочих груп, які створюються для вирішення окремих питань. Незважаючи на це, з огляду на різні стратегічні та оперативні потреби, якщо немає чіткої політичної директиви, розроблені рекомендації та варіанти реагування на кризи часто базуються на загальних мінімальних стандартах. Такий вузький функціональний підхід часто не дає змоги знайти відповіді в складних і мінливих обставинах. По-друге, існує проблема перетворення результатів політичних і урядових рішень на процеси, які мотивують і мобілізують громадян на досягнення спільних цілей, як-от створення та підтримка стійких інформаційних екосистем.

Настав час запровадити інший підхід, в межах якого основна відповідальність покладається на підтримання стійкості суспільства в цілому, а також заохочується більша гнучкість. Не дублюючи оперативні функції, які вже виконують державні органи, спеціальна національна інституція, створена на підставі рішення парламенту, могла б стати важливою опорою критичної демократичної інфраструктури (див. 3.3: Ролі та обов'язки), об'єднуючи різні зусилля по всій країні. До її повноважень та основних функцій могли б належати: керування розвитком знань та доказів для покращення розуміння стану національної інформаційної екосистеми, включно із загрозами та ризиками, розробка підходу, що охоплює все суспільство, шляхом консультацій та формування стандартів, забезпечення уніфікованої розбудови спроможності, виявлення та попередження нових проблем шляхом мобілізації ресурсів та експертних знань, а також співпраця з урядом, бізнесом та неурядовими організаціями з метою підвищення цілісності та стійкості інформаційної екосистеми шляхом впровадження регулювання та всебічних політичних рекомендацій. Таким чином, ця установа буде виконувати роль сполучної ланки між горизонтальною та вертикальною осями державного управління та реалізації політики.

Нижче наведено три популярні концептуальні моделі, які часто застосовуються в демократичних країнах для протидії новим загрозам в інформаційному середовищі. Цей стислий аналіз може бути корисним для читачів, які розглядають досвід різних країн, включаючи сфери повноважень таких спеціалізованих установ.

3.2.1. **Національна безпека**

Що стосується операцій іноземного втручання, багато демократичних країн висловлюють подібні занепокоєння щодо надмірного впливу радикальних або екстремістських угруповань, спроб впливу на вітчизняних політиків з боку іноземної держави, кібератак на критичну інфраструктуру або загроз безпеці виборів. Правомірно визнаючи ці зловмисні дії загрозами національній безпеці, представники політичної влади та уряди традиційно дотримуються двох взаємопов'язаних курсів дій. По-перше, вони підвищують обізнаність громадськості стосовно нових загроз та мобілізують громадську думку на підтримку дій уряду. До таких дій найчастіше належать моніторинг та спостереження, обмін оперативно-аналітичними і розвідувальними даними, правоохоронні заходи, що підкріплюються відповідними законодавчими та регуляторними заходами. Важливу роль у цих зусиллях відіграють також стратегічні комунікації. По-друге, уряди вживають зусиль для створення нових або реорганізації наявних механізмів протидії загрозам. Однак ці зусилля часто є розрізненими, що зумовлено технічними, політичними та оперативними обмеженнями, а також масштабом і обсягом визначеної проблеми.

Описаний вище функціональний підхід передбачає реагування на виявлені загрози та дає урядам можливість застосовувати традиційні методи захисту національної безпеки. Чинні нормативно-правові рамки, повноваження та процеси поширюються на нові безпекові загрози, водночас за необхідності усуваються наявні прогалини. Водночас, як свідчать останні дані, цей підхід виявляє низку прогалин на таких рівнях:

1. *Концептуальний*. Вирішення однієї або декількох інформаційних проблем ізольовано від інших суперечить системній природі сучасного інформаційного середовища.

2. *Стратегічний*. Пасивний підхід, в основі якого лежить реагування на загрози, унеможливлює формування цілісної національної інформаційної екосистеми на засадах демократичних цінностей і принципів — такої, що мобілізуватиме усі наявні ресурси і даватиме поштовх до проактивних дій.

3. *Операційний*. Незважаючи на покращення деяких функцій, такий підхід може збільшити інституційні бар'єри (зокрема, контроль з боку правоохоронних органів) та операційні витрати (як-от координація), а це позначиться на ефективності управління.

4. *Суспільний*. Може бути складно мобілізувати підтримку та участь публіки через гостру поляризацію суспільства та низький рівень довіри до державних інституцій та ЗМІ.

3.2.2. **Тотальна оборона**

Ця концепція, яка переважно застосовується в скандинавських країнах Європи, а також у Сінгапурі та Швейцарії, поєднує загальносуспільні та

загальнодержавні підходи до національної безпеки та захисту від загроз (Nicholson et al. 2021; Berndtsson 2024; Palmertz et al. 2024). Підкреслюючи готовність та стійкість країни до військових і невійськових загроз, ця концепція передбачає системний підхід до організації ресурсів і спроможностей країни. Основна увага приділяється формуванню у населення готовності чинити опір і, за необхідності, давати відсіч, що виявляється у формуванні спільного розуміння реальної ситуації та спільної мети серед усіх зацікавлених сторін, включаючи окремих громадян, компанії та усі рівні влади. Хоча загрози та ризики можуть виявлятися у багатьох непередбачуваних формах (наприклад, природні катастрофи, пандемії або гібридні атаки), здатність суспільства забезпечити безперебійність послуг та виживання залежить від психологічної готовності його громадян.

Основна увага приділяється культивуванню у населення готовності чинити опір і, за необхідності, давати відсіч.

Завдяки більш системному та стратегічному підходу ця концепція відкриває шлях для формування відповідних наративів, процесів, спроможностей та регулювання, водночас залучаючи та мотивуючи все суспільство. Таким чином, концепція тотальної оборони має все необхідне для того, щоб подолати прірву між різноспрямованими організаційними, інституційними та мотиваційними цілями і завданнями. Окрім того, це надає можливість окреслити ціннісні орієнтири, надзвичайно необхідні для становлення поколінь, нації та формування ідентичності. Однак слід зазначити, що багато юрисдикцій, які йдуть цим шляхом, вже мають вищий рівень суспільної згуртованості або завдяки історично сформованому почуттю спільної ідентичності, або завдяки здатності використовувати наявні геополітичні чи безпекові умови, а також фундаментальні культурні та соціальні норми. Більш складно буде реалізувати цю концепцію в мультикультурних демократичних суспільствах, де громадяни мають різні уявлення про інформаційні загрози або розбіжні погляди на соціальні та політичні пріоритети в більш широкому сенсі.

3.2.3. **Захист цілісності інформації**

Останнім часом Організація Об’єднаних Націй запропонувала нову комплексну концепцію для створення та підтримання здорових інформаційних екосистем. Для цього потрібна ретельна координація дій. Визнаючи негативний вплив маніпуляцій або інформації низької якості на вибір, який робить людина, її права і свободи, приватність та безпеку, ООН окреслила нарис майбутньої глобальної концепції, а також рекомендації для різних національних суб’єктів (United Nations n.d.; Bentzen 2024). Вони заохочують зацікавлені сторони дотримуватися належних практик у сфері цифрової політики, управління цифровими платформами, внутрішньої резистентності та протидії дезінформації (Government of Canada 2024; OECD 2024b).

Створення національних інформаційних екосистем, що базуються на точній, послідовній, надійній та захищеній від підробок інформації, яка дає змогу приймати рішення як на індивідуальному, так і на організаційному рівні, — це візійна ідея в епоху інформації. Цю концепцію

можна реалізувати як спільну мету, щоб надати фізичним особам, організаціям та суб'єктам прийняття рішень змістовні рекомендації для оцінки їхньої індивідуальної та інституційної діяльності. Зокрема, у межах Програми розвитку ООН було розроблено кілька посібників та рамкових документів з метою захисту цілісності інформації під час виборчих циклів та поза ними (Центр політики управління ПРООН, без дати). Ця концепція може бути реалізована у межах наявної системи громадської безпеки та національного управління надзвичайними ситуаціями (у поєднанні з підходом тотальної оборони) (Adam et al. 2023). Оскільки глобальне інформаційне середовище є спільним для всіх, ця

Блок 3.2. **Заходи Іспанії щодо протидії дезінформації**

Визнаючи загрозу національній безпеці та суспільству, у 2019 році Іспанія створила національний орган під головуванням президента для розробки та координації державних заходів (Government of Spain, 2020). Цей механізм, який очолює Департамент національної безпеки (Departamento de Seguridad Nacional, DSN) та який функціонує як Постійний комітет з протидії дезінформації, забезпечує координацію діяльності різних урядових органів з метою виявлення кампаній з дезінформації, інформування громадськості, підтримки урядових рішень з відповідних питань та координації національних заходів реагування. Такий підхід сприяє обміну інформацією між органами, відповідальними за виявлення та аналіз загроз, а також комунікацію і дипломатію. Окрім того, це дає змогу представникам різних зацікавлених сторін розвивати співпрацю на робочому рівні, формувати горизонтальні зв'язки, що є особливо цінним, коли є потреба згуртуватися для реагування на загрози.

Ці заходи на національному рівні формуються відповідно до актуальних ініціатив Європейського Союзу, як на стратегічному, так і на тактичному рівні. Наприклад, нещодавно уряд прийняв рішення про розробку комплексної національної стратегії боротьби з дезінформацією, що включає такі заходи, як збір пропозицій від громадськості щодо способів боротьби з дезінформацією (Government of Spain 2020). Спираючись на керівні принципи ЄС, а саме на Європейський план дій з питань демократії 2020 року, у рішенні окреслено ключові ролі та очікування щодо дієвої національної стратегії, в основі якої лежить контекстуальний аналіз та фактологічні дані, а також мета «[досягти] якомога ширшого консенсусу між залученими сторонами».

Визнаючи, що взаємодія з громадянським суспільством, ЗМІ та іншими зацікавленими сторонами є запорукою внутрішньої резистентності, Департамент національної безпеки прагне налагодити партнерські відносини між приватним і державним секторами шляхом консультацій, сприяння науковим дослідженням тощо (Government of Spain, 2025a). Одним із результатів цієї діяльності стало створення громадського Форуму проти кампаній з дезінформації у сфері національної безпеки (Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional) як консультативного органу для просування загальносуспільного підходу, відповідних робочих груп та публікацій. Започаткований у 2022 році, цей форум об'єднав понад 100 експертів з академічних кіл, аналітичних центрів, засобів масової інформації, цифрових компаній та НУО. Щороку Департамент національної безпеки публікує звіт про ініціативи, реалізовані в межах форуму.

> [Форум як] простір для співпраці між державними установами та громадянським суспільством, приватним сектором та науковими колами утвердив свою позицію як надійний інструмент обміну знаннями про ризики, які дезінформація становить для нашої демократії та верховенства права. Він також заохочує дискусію про наявні механізми протидії цим загрозам. Він об'єднує представників основних секторів суспільства, які займаються виявленням, аналізом та мінімізацією загроз.
> —Лорето Гутьєррес Уртадо, директор Департаменту національної безпеки та голова Форуму проти кампаній з дезінформації у сфері національної безпеки (Уряд Іспанії 2025b: Вступ).

концепція може максимально пов'язати питання внутрішнього розвитку та національної безпеки з більш універсальною програмою «глобального суспільного блага», основою якої є рішуча відданість захисту прав людини, демократичних цінностей та принципів. Це можна потенційно перетворити на дієві національні інструменти шляхом підвищення обізнаності та розробки практичних рекомендацій на основі аналізу інформаційної екосистеми та консультацій із зацікавленими сторонами.

Питання, на які слід надати відповідь, окреслюючи повноваження інституції, відповідальної за збереження доброчесності інформації:

- Які конкретні прогалини в нинішніх інституційних підходах ця установа могла б заповнити? Зокрема це стосується координації та обміну інформацією між урядовими та неурядовими суб'єктами?
- Як інституція забезпечуватиме легітимність та довіру серед стейкхолдерів, особливо в контроверсійних питаннях?
- Якими принципами вона керуватиметься у взаємодії із зацікавленими сторонами, враховуючи наявні протиріччя, балансуючи між прозорістю, безпекою та плюралізмом? Як вона забезпечуватиме виконання своїх рекомендацій щодо політично контроверсійних питань?
- Як інституція має балансувати між тим, щоб реагувати на нові загрози та тим, щоб забезпечувати сталий довгостроковий розвиток суспільства?
- Як уникнути дублювання функцій та конфлікту повноважень?

3.3. **РОЛІ ТА ОБОВ'ЯЗКИ**

У цьому розділі коротко викладено основні функції, які може виконувати національна установа, відповідальна за збереження доброчесності інформації. Підкреслимо, що до чільних завдань цієї установи належать організація та координація діяльності різних суб'єктів у сфері збереження цілісності інформації. Діяльність інституції повинна базуватися на передовому досвідові демократичних країн, які вже застосовують загальносуспільні та загальнодержавні підходи. Об'єднання таких функцій в межах однієї національної установи також може сприяти кращій міжнародній координації.

1. *Координаційна функція*. Інституція могла би мобілізувати ресурси та координувати загальнодержавний та загальносуспільний підхід до забезпечення цілісності національної інформаційної екосистеми відповідно до демократичних цінностей та принципів. Це сприятиме забезпеченню резистентності суспільства до інформаційних загроз. Залежно від того, яке місце буде відведено цій установі у структурі державного управління, її обов'язки можуть включати керування, розроблення та координацію заходів. Одним із прикладів такої координації можуть бути національні виборчі цикли. Якщо ця державна установа буде позиціонуватися як така, що перекидатиме місток від інтересів державних установ до неурядових організацій, вона буде відігравати важливу роль координатора, виявляти прогалини та ініціювати міжвідомчу або багатосторонню співпрацю,

зокрема у форматі міжнародного співробітництва[6]. Як національний лідер інформаційної екосистеми, ця організація матиме також певну, хоча дещо обмежену, роль у виявленні системних прогалин, розробці концепцій та рекомендацій, розбудові спроможності та оптимізації інформаційних потоків. Проте розроблення та реалізація оперативних заходів залишатимуться прерогативою відповідних органів, як-от Міністерства закордонних справ, Міністерства оборони чи Міністерства внутрішніх справ.

2. *Консолідація стейкхолдерів*. Враховуючи численні суспільно-політичні ризики та вразливості, а також еволюцію гібридних загроз, для цієї установи буде вкрай важливо налагодити співпрацю з вітчизняними суб'єктами та іноземними партнерами. Усередині країни може бути створена національна консультативна рада, до складу якої входитимуть експерти з уряду, громадянського суспільства та наукових кіл. Вони проводитимуть регулярні зустрічі з метою виявлення вразливостей у внутрішній інформаційній екосистемі та розробки рекомендацій щодо подолання цих проблем (рекомендації матимуть спонукальний характер «м'якого права»)[7]. Деякі із зазначених нижче обов'язків також можуть бути реалізовані завдяки довгостроковим програмам, що фінансуються за участю громадянського суспільства та академічних партнерів (наприклад, розбудова спроможності, моніторинг або дослідження). На міжнародному рівні це може передбачати тісне партнерство з подібними національними інститутами для просування узгодженого, демократичного підходу до глобального інформаційного середовища, відповідно до демократичних цінностей і принципів.

3. *Моніторинг та аналіз інформаційної екосистеми*. Як незалежна національна установа, ця організація має виявляти та аналізувати загрози в інформаційному середовищі. Визначення факторів та умов, що впливають на зміни в національній інформаційній екосистемі, включаючи загрози та тенденції, допоможе всім зацікавленим сторонам згуртуватися та спільно протистояти таким загрозам. Цей аналіз і оцінка загроз може здійснюватися на двох рівнях: стратегічний рівень передбачає аналіз суспільно-політичних, правових, економічних, культурних, регуляторних, безпекових та інших чинників і тенденцій, що впливають на всю екосистему; оперативний рівень передбачає моніторинг еволюції інформаційних загроз. Виконані цією установою дослідження, які будуть виходити за рамки звичайного огляду традиційних ЗМІ і соціальних мереж, слугуватимуть підґрунтям для прийняття системних регуляторних, правових та політичних рішень, а також для створення інфраструктури та залучення необхідних ресурсів. Аналіз загроз може бути виконаний у співпраці з партнерами з громадянського суспільства та урядовими установами. Наразі переважна частина

---

[6] Попередній досвід забезпечення кібербезпеки під час виборів може стати цінним прикладом (див. Van der Staak і Wolf 2019).

[7] Довідкова інформація доступна у переліку використаних джерел, див. Polish Ministry of Foreign Affairs (2025) та Alkema (2025). Для ознайомлення з конкретними прикладами взаємодії із зацікавленими сторонами див. Van der Staak і Wolf.

Виявлення загроз, тенденцій та факторів впливу на національну інформаційну екосистему допоможе згуртувати зусилля зацікавлених сторін для протидії маніпулятивному дискурсу.

такого моніторингу здійснюється державою. Вочевидь, державні установи з міркувань безпеки бажатимуть продовжити виконувати такий моніторинг, бодай частково. Зауважимо, що прозорість та суспільна довіра до аналітичних доповідей стосовно загроз була би істотно вищою, якби до їх підготування були б залучені іноземні експерти та експертні спільноти. Це також допомогло би підвищити загальний рівень обізнаності громадськості та стійкості під час виборчих циклів та поза ними[8]. Зусилля такої інституції можуть бути направлені на розробку протоколів обміну інформацією між вітчизняними установами, що займаються збором і обробкою оперативно-аналітичних і розвідувальних даних, виборчими комісіями, ЗМІ та незалежними організаціями громадянського суспільства. Це допомогло би сформувати більш комплексну картину загроз та підвищити довіру до демократичних процесів та управління в цілому.

4. *Накопичення знань та розбудова спроможності*. Національна установа з питань захисту доброчесності інформації повинна мати спроможність підтримувати партнерські відносини з академічними спільнотами, аналітично-дослідницькими центрами, медійними та громадськими організаціями, а також слугувати національним центром акумулювання та поширення знань, проведення інформаційно-просвітницьких кампаній. Інформаційно-просвітницька робота сприятиме виробленню кращого суспільного розуміння критичних факторів, що впливають на інформаційну екосистему. Водночас це дасть змогу виявляти тренди та прогалини, а також пропонувати можливі рішення. Така установа могла би сприяти узгодженому та послідовному розвитку навичок, спроможностей і знань у державному та громадському секторі шляхом підтримання партнерських відносин, зокрема за допомогою цільового довгострокового фінансування досліджень для формування державної політики, розробки технічних інструментів та навчальних модулів. Ця спеціалізована державна установа могла би координувати підготовку, стандартизацію і проведення навчальних програм і тренінгів для різних суб'єктів у партнерстві з представниками громадянського суспільства.

5. *Комунікація*. Спеціалізована державна установа з питань захисту доброчесності інформації матиме всі можливості для активного формування публічного діалогу щодо викликів, прогалин та майбутнього сучасного інформаційного суспільства. Таким чином, ця незалежна державна установа сприятиме розвитку важливих суспільних відносин, як описано вище. Безумовно, це залежить від наявності відповідних політичних умов та від того, чи вдасться

[8] Багато країн вже беруть участь у таких спільних заходах з моніторингу, бодай у форматі короткострокових проєктів. Такі моніторингові зусилля можуть бути істотно покращені за рахунок використання стандартизованих протоколів (наприклад, Structured Threat Information Expression) та узгоджених дефініцій (наприклад, DISARM Framework), що забезпечить обмін належним чином структурованими даними. Щоб отримати додаткову інформацію, радимо звернутися до Центру інформації стосовно маніпулювання дискурсом та втручання в інформаційну сферу з-за кордону (FIMI-ISAC).

їй отримати широку суспільну довіру. За такої умови вона зможе істотно зменшити виклики, що стоять перед урядовим органом у сфері стратегічних комунікацій. Це особливо актуально для державної служби, де зазвичай здійснюються всі можливі зусилля для мінімізації ризиків. У дуже динамічному та насиченому подіями інформаційному просторі кожна інформаційна прогалина стає можливістю для зловмисників заповнити її дезінформацією або маніпулятивним дискурсом. Така інституція могла би сприяти виробленню нових норм і формуванню державної політики, пропонуючи різного роду звіти і рекомендації, розроблені завдяки співпраці і партнерській взаємодії між різними сторонами. Обов'язковою умовою є дотримання принципів прозорості, доступності, доказовості.

Блок 3.3. **VIGINUM — Служба протидії іноземним втручанням у сфері цифрових ЗМІ, Франція**

Створена у 2021 році за указом президента Франції, Служба протидії іноземним втручанням у сфері цифрових ЗМІ — VIGINUM (Service de vigilance et protection contre les ingérences numériques étrangères) є органом, що виконує оперативно-аналітичні і технічні функції. Повноваження цього органу полягають у виявленні та аналізові іноземних втручань у цифровій сфері. Цей орган займається такими атаками, що спрямовані на підрив національних інтересів Франції. Працюючи винятково з відкритими джерелами інформації, VIGINUM аналізує комплекси інформаційно-маніпуляційних операцій, виявляє та відстежує тактики, прийоми та процедури, що застосовуються іноземними суб'єктами, а також підвищує обізнаність щодо інформаційних загроз серед молоді, громадськості, медіа та урядових установ (VIGINUM n.d.; див. також Уряд Франції 2021).

Ця Служба увійшла до структури Генерального секретаріату з питань оборони та національної безпеки (Secrétariat général de la défense et de la sécurité nationale) при Прем'єр-міністрові Франції. Вона забезпечує координацію діяльності Міністерства Європи та закордонних справ, Міністерства збройних сил і Міністерства внутрішніх справ. Працюючи винятково як слідчий орган, вона не займається виправленням недостовірної інформації. Служба дотримується суворих правил збору та зберігання відкритих даних, щоб гарантувати відповідність вимогам законодавства у сфері захисту приватності й етики та уникнути сприйняття її діяльності як стеження за громадянами. З 2024 року служба співпрацює з французьким регуляторним органом з питань цифрових комунікацій (Autorité de régulation de la communication audiovisuelle et numérique, Arcom), надаючи технічну підтримку для впровадження Закону ЄС про цифрові послуги.

Служба VIGINUM виконує моніторинг інформаційно-цифрової сфери за поведінковими індикаторами, що пов'язані з ворожими мережами та інфраструктурою. Такий моніторинг покращує здатність цього органу виявляти нові загрози та забезпечувати раннє попередження для ширшого кола зацікавлених осіб. Ключовими напрямками діяльності є розбудова спроможності та підвищення обізнаності цілої низки різних суб'єктів і зміцнення співпраці з міжнародними партнерами з метою кращої координації заходів реагування.

> Необхідно сприяти формуванню єдиної європейської та міжнародної культури боротьби з маніпулюванням інформацією. Вона повинна бути зосереджена на досягненні трьох цілей: стандартизації практик виявлення, посиленні можливостей виявлення в цільових країнах та сприянні взаємодії між державами та всією спільнотою, залученою до боротьби з маніпулюванням інформацією. Насамкінець, необхідна краща координація між державним і приватним сектором і громадянським суспільством, щоб гарантувати узгодженість наших дій та посилити стійкість суспільства.
> —Марк-Антуан Бріллант, керівник департаменту, VIGINUM

Питання щодо ролей та обов'язків спеціалізованої установи із захисту доброчесності інформації:

- Які ключові функції має виконувати установа, щоб виступати авторитетним національним центром захисту і гарантування стійкості інформаційної екосистеми?
- Яку роль установа може відігравати у балансуванні нових пріоритетів і підходів у нових сферах суспільного інтересу (поза межами офіційної політики) та об'єднанні зусиль міжнародних партнерів — організацій з державного та недержавного сектора?
- Яку роль установа повинна відігравати у проведенні регулярних оглядів національної інформаційної екосистеми та формуванні суспільного попиту на замовлення таких аналітичних продуктів?
- Які умови слід визначити для зацікавлених сторін з метою досягнення спільних результатів, впровадження вироблених рекомендацій або врегулювання розбіжностей? Як керувати очікуваннями різних суб'єктів?

3.4. **ОРГАНІЗАЦІЙНА СТРУКТУРА**

Традиційно організаційна структура тлумачиться як сукупність елементів, що представляє політику організації, ролі та обов'язки посадових осіб, моделі управління, а також внутрішньоорганізаційні та міжорганізаційні відносини відповідно до виконуваних установою функцій. У цьому дискусійному документі ми вже висвітлили деякі з аспектів організаційної структури такої спеціалізованої установи із захисту доброчесності інформації. Безумовно, у кожному конкретному випадку організаційна структура подібних організацій визначається залежно від національного контексту, політичного ландшафту і практичних обмежень, проте ми розглядаємо це питання з більш системного, загальносуспільного погляду.

Аби розробити і впровадити нові механізми управління, потрібна велика політична воля для координації різних суб'єктів, процесів і ресурсів для підтримки відповідних інформаційних потоків та прийняття рішень. Політичне керівництво країни, прагнучи досягнути мети створення стійкої системи протидії інформаційним загрозам, незалежної від їх виду, повинні заохочувати єдність і співпрацю різних суб'єктів з метою налагодження організаційних процесів та забезпечення бажаного результату.

Одним з ключових викликів на цьому шляху є координація процесів і суспільно-політичних відносин, які можуть бути одночасно сталими і гнучкими. З одного боку, гнучкість важлива для систем управління, щоб мати змогу реагувати на непередбачувані, нелінійні форми соціально-політичних і геополітичних змін. З іншого боку, така спеціалізована установа із захисту доброчесності інформації повинна буде керувати поточними ініціативами та просувати нові методи, одночасно забезпечуючи їхнє достатнє вкорінення для досягнення бажаних результатів. Для цього її робота повинна базуватися на високому професіоналізмі, глибокій обізнаності в політичних та технічних питаннях, прозорій організаційній поведінці, повазі до фундаментальних прав та етичних стандартів, а також на визнаному лідерстві та інших визначальних характеристиках. Подібним чином, з огляду на велику

кількість чутливих питань, як-от національна безпека та оборона, а також достатню потенційну впливовість на національному рівні, інституція повинна, з одного боку, підтримувати відносини з виконавчою та законодавчою гілками влади, а з іншого боку — взаємодіяти з різними зацікавленими сторонами. Дотримуючись таких принципів, а також підтримуючи репутацію чесного посередника, така спеціалізована установа матиме всі підстави і важелі впливу для забезпечення міжвідомчої та міжгалузевої співпраці. Своєю чергою, це забезпечить міцну основу для вироблення спільних принципів і практик.

На практиці організаційна структура такої спеціалізованої установи залежатиме від її мандату та виконуваних нею функцій, а це, своєю чергою, потребуватиме аналізу необхідних навичок, рівня професійного стажу та експертного досвіду її співробітників. Усі функціональні команди повинні мати високий рівень спільного усвідомлення мети (на горизонтальному рівні), одночасно зосереджуючись на досягненні конкретних результатів. Для цього потрібно мати надійну комунікаційну платформу всередині організації та систему управління проєктами. Якщо залучення всього суспільства стане однією з інституційних цілей, то найбільш продуктивним може виявитися застосування мережевого підходу до розподілу обов'язків і функцій. Це дасть змогу зробити організаційну структуру такої установи більш компактною та прозорою. Як зазначалося раніше, такий підхід має сприяти більшій довірі та підтримці з боку всіх зацікавлених сторін.

Перший етап розроблення детальної карти суб'єктів та проєктів, а також різних потреб, можливостей та прогалин на національному рівні дасть змогу ідентифікувати всіх причетних суб'єктів та розробляти робочі плани. Таким чином, це допоможе систематизувати відповідні методи роботи і залучення партнерів до реалізації заходів, чи то шляхом фінансування моніторингу інформації з відкритих джерел, чи то шляхом створення робочих груп. Безумовно, з огляду на численні виклики, створення цієї організації та забезпечення функціонування її мереж не буде простим завданням. Гнучкість та експериментальність залишатимуться як головними характеристиками, так і вимогами до її персоналу та усіх запущених процесів. Підтримання загальносуспільного підходу та життєдіяльності інституції потребуватиме постійних зусиль для підвищення колективного розуміння того, як формувати стійкі внутрішні екосистеми відповідно до демократичних цінностей та цілей.

Питання стосовно організаційної структури:

- Яка модель організаційної структури забезпечить гнучкість, інклюзивність та довіру зацікавлених сторін? Прикладами можуть бути постійний секретаріат, ротаційні панелі, тематичні робочі групи.
- Як призначати керівництво та забезпечувати державне фінансування таким чином, щоб гарантувати незалежність від виконавчої влади або політичного впливу?
- Які внутрішні спроможності (наприклад, аналітичні, юридичні, технічні) необхідні для того, щоб організація якнайкраще виконувала свої повноваження?
- Як слід організувати та документувати процеси прийняття рішень та надання рекомендацій, щоб забезпечити прозорість, підзвітність та ефективність?

Блок 3.4. **Центр стратегічних комунікацій та протидії дезінформації Молдови**

В умовах систематичних російських гібридних операцій, зокрема інформаційних атак (EUvsDisinfo 2025), у 2023 році Молдова заснувала Центр стратегічних комунікацій та протидії дезінформації. Центр було створено на підставі рішення парламенту. Одне з його ключових завдань полягає у консолідації та покращенні координації між урядовими установами, відповідальними за конкретні аспекти боротьби з маніпулюванням інформацією та іноземним втручанням, як-от Рада з питань аудіовізуальних засобів масової інформації, Служба безпеки та інформації, Координаційна рада із забезпечення інформаційної безпеки та Національне агентство з кібербезпеки.

Одним із перших результатів його діяльності стала «Концепція стратегічних комунікацій та протидії дезінформації, маніпуляціям інформацією та іноземному втручанню на 2024—2028 роки». Відповідно до цілей Національної стратегії безпеки, концепція визначила різні форми маніпулювання інформацією та втручання як загрози і ризики для національних інтересів, визнала вразливість системи управління та запропонувала конкретні заходи для забезпечення національної безпеки та стійкості відповідно до демократичних принципів (Парламент Республіки Молдова, 2023). З моменту свого створення Центр продовжує випробовувати та впроваджувати різні практики, співпрацюючи з урядовими установами, громадянським суспільством та приватним сектором.

Центр стратегічних комунікацій та протидії дезінформації Молдови зосереджується на підвищенні стійкості суспільства до інформаційних загроз, які здійснюють негативний вплив на життя, цінності людей та національну безпеку. Проактивні та превентивні заходи забезпечення стійкості вимагають проведення оцінки загроз та вразливостей на постійній основі, а також вивчення громадської думки з різних питань, а також заходів, спрямованих на підвищення довіри до демократичних інституцій, цінностей та практик. Водночас політичні лідери та суб'єкти прийняття рішень повинні визнати, що формування загальносуспільного підходу щодо підвищення стійкості до інформаційних загроз є довготривалим процесом. Такі суб'єкти мають комунікувати не лише державну позицію та інтереси уряду, а й надавати можливість висловити критичну думку всім охочим, як у період виборчих циклів, так і поза ними, щоб подолати розбіжності в сприйнятті та побудувати довіру.

> Політичні еліти в демократичних суспільствах мають визнати, що інформаційні загрози необхідно розглядати як складову планування національної безпеки. Це відкриває шляхи для розвитку та організації проактивних зусиль у взаємодії між усіма національними суб'єктами та у співпраці з міжнародними партнерами з метою досягнення спільних національних інтересів.
> —Ана Ревенко, директорка Центру стратегічних комунікацій та протидії дезінформації, Республіка Молдова

3.5. **НАГЛЯД**

З огляду на різні проблеми, очікування, а також ризики у сфері суспільно-політичних відносин та безпеки, спеціалізована національна установа, що займається захистом доброчесності інформації, потребуватиме ефективного нагляду з боку суспільства. Забезпечення прозорості та підзвітності у діяльності цієї установи також зменшить можливі ризики, пов'язані з уявленням про державний контроль, загрози основним правам людини або політичну упередженість. У цьому контексті діяльність цієї інституції могла б регулювати наглядова рада. До складу цієї наглядової ради могли би входити представники уряду, громадянського суспільства, наукових кіл та бізнесу. Наглядова

рада могла би надавати дорадчу підтримку керівництву організації та готувати щорічні звіти. Членів наглядової ради можна було би обирати на основі їхньої професійної компетентності та досвіду роботи на державній службі. Строки їхніх повноважень можна регулювати так, щоб оновлення складу ради відбувалося поетапно, з метою забезпечення безперервності роботи та поступового оновлення складу ради. Процедури висування кандидатур та відбору повинні бути організовані та проводитися прозоро та з фіксацією результатів.

Наглядова рада може презентувати щорічні звіти у законодавчому органі для забезпечення суспільного контролю. Такі звіти мають висвітлювати характер і масштаби проведених заходів, оприлюднювати статистичні дані, інформацію про призначення персоналу та різні інші питання, як-от отримані скарги та механізми правового захисту. Ці звіти дадуть змогу забезпечити достатній рівень прозорості і підзвітності, а це сприятиме розбудові суспільної довіри до цієї спеціалізованої організації та мінімізації можливого негативного сприйняття. Регулярне залучення традиційних і нових медіа до висвітлення діяльності інституції слугуватиме додатковим інструментом інформування громадськості про її роботу.

З адміністративного погляду, внутрішня діяльність інституції може регулюватися чинною нормативно-правовою базою та правовими інструментами.

Питання щодо нагляду:

- Які механізми допоможуть забезпечити прозорість та підзвітність у діяльності такої спеціалізованої установи, що слугуватиме гарантією легітимності її дій?
- Хто повинен мати повноваження виконувати оцінку діяльності такої спеціалізованої установи?
- Яким чином організувати нагляд у найбільш ефективний спосіб, щоб уникнути домінування політичних інтересів певних груп або надмірної політизації?
- Яку роль у нагляді над діяльністю такої спеціалізованої установи відіграють парламент, незалежні органи чи громадянське суспільство?
- Як слід вбудувати в діяльність інституції механізми зворотного зв’язку для забезпечення постійного вдосконалення?

3.6. **МІЖНАРОДНА КООРДИНАЦІЯ**

Хоча в цьому документі обговорювалися питання, пов'язані з внутрішньою координацією, важливо підкреслити, що належним чином організовані внутрішні заходи сприятимуть комплексному демократичному підходу до інформаційних загроз. Багато країн вже обмінюються передовим досвідом, інформацією та координують відповідні заходи в рамках урядових ініціатив, як-от Механізм швидкого реагування G7, Європейська система швидкого оповіщення, Організація Північноатлантичного договору (НАТО), Організація економічного співробітництва та розвитку та інші. Проте, незважаючи на їхню корисність у багатьох аспектах, значна частина цих ініціатив стикаються з труднощами у координації зусиль через різні контексти, правові та регуляторні рамки, рівні обізнаності, ізольовані підходи, різні спроможності та обмеженість повноважень. Послідовність, швидкість та ефективність реакції демократичних країн на неспровоковану війну Росії в Україні продемонстрували численні прогалини в наявних підходах. Водночас цей здобутий досвід відкриває можливості для вдосконалення стратегій і операційної спроможності.

Багато представників владних структур, що були опитані у межах підготовки цього дискусійного документа, визначили подібні прогалини у внутрішній та міжнародній координації. На багатьох рівнях ці прогалини зумовлені двома ключовими аспектами — людським (різний рівень обізнаності та можливостей) та організаційним (жорстка та ієрархічна організація управління інформацією). Швидкоплинні зміни в операційному та безпековому середовищі ставлять серйозні виклики перед урядами, які бажають вирішити ці аспекти більш оперативно.

Державні установи, залучені до міжвідомчої взаємодії і співпраці з іншими органами виконавчої влади і громадськими організаціями, могли би виступати в ролі інституційних посередників між різними суб'єктами. Вирішуючи операційні, політичні та репутаційні проблеми, вони могли би сприяти більш відкритому діалогу. У центрі такого діалогу можуть бути фундаментальні питання формування знань, розробки технологічних інструментів або методів. Це дасть змогу забезпечити оперативну досконалість та розбудовувати спроможність урядових органів[9]. Водночас цінними можуть стати зусилля з боку неурядових організацій, які потенційно можуть допомогти розробити і випробувати новітні підходи як у галузі політики, так і на практиці для забезпечення колективної обізнаності, стійкості та цілісності інформації.

У міру розвитку цих відносин у демократичних країнах наступним кроком може стати створення спільних ініціатив, які стануть частиною глобальної демократичної критичної інфраструктури. Демократичні країни зміцнюватимуть колективну резистентність та сприятимуть

[9] Створення FIMI–ISAC може слугувати зразком того, як різні суб'єкти можуть налагоджувати або посилювати співпрацю.

доброчесності інформації в усьому світі шляхом координації фінансування, розбудови спроможності, підвищення обізнаності суспільства.

Питання щодо міжнародної координації:

- З якими міжнародними партнерами або коаліціями ця установа повинна співпрацювати і на яких умовах?
- Чи існують конкретні прогалини в комплексних діях урядів, вжитих з метою підвищення стійкості суспільства, розбудови спроможності або обміну інформацією, наприклад, у питаннях управління штучним інтелектом, кіберстійкості або протидії іноземній інформаційній маніпуляції та втручанню (FIMI)? Ці прогалини є такими, які могла би заповнити співпраця з подібними інституціями в інших країнах.
- Яку роль ця установа могла б відігравати у розробці комплексного демократичного підходу разом з іншими подібними організаціями? Як би це допомогло виявити спільні прогалини та можливості для сталого розвитку здорових інформаційних екосистем?

3.7. **ТЕОРІЯ ЗМІН ДЛЯ ЗАХИСТУ НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ ЕКОСИСТЕМ**

У цьому блоці пропонується розглянути перспективу можливого сценарію майбутнього розвитку. Тут розглядається, як імовірні сценарії розвитку та дії, запропоновані в цьому дискусійному документі, можуть забезпечити досягнення цілого ланцюга результатів, що сприятимуть сталому і стійкому розвитку державної політики і демократичного суспільства. Інформація подається структуровано відповідно до звичної форми теорії змін.

1. **Якщо** демократичні уряди та суспільства визнають, що фрагментоване, ізольоване реагування на інформаційні виклики та загрози, як-от дезінформація, іноземне втручання та зловживання новими технологіями, є недостатніми для захисту доброчесності їхніх національних інформаційних екосистем,

   то вони повинні створити спеціалізовану національну установу, яка виступатиме стратегічним координаційним центром для аналізу, координації та розробки рекомендацій у різних галузях.

2. **Якщо** така спеціалізована національна установа матиме можливість проводити постійний аналіз національної інформаційної екосистеми, включаючи виявлення вразливостей, прогалин та тенденцій,

   то вона зможе генерувати своєчасні, засновані на фактологічних даних висновки, які слугують основою для розробки державної політики, допомагають урядовим установам і неурядовим організаціям в прийнятті рішень.

3. **Якщо** ця спеціалізована національна установа об'єднуватиме різні суб'єкти — урядові органи, громадянське суспільство, наукові кола, бізнес — в рамках інклюзивних форумів та робочих груп,

   то вона зможе сприяти підвищенню спільної обізнаності, зміцненню довіри та узгодженню зусиль, які наразі є розрізненими або суперечливими.

4. **ЯКЩО** установа сприяє обміну знаннями та розбудові спроможності завдяки семінарам та іншим інструментам,

   то зацікавлені сторони будуть краще підготовлені до реагування на нові виклики та загрози, впровадження системніших практик та демократичних процедур у свої підходи.

5. **ЯКЩО** інституція надає рекомендації, що не мають зобов'язувального характеру, та виступає посередником між внутрішніми та міжнародними суб'єктами,

   то вона зможе підтримувати узгоджені національні стратегії, одночасно сприяючи глобальній демократичній стійкості, не порушуючи суверенітету чи громадянських свобод.

6. **ЯКЩО** уряди зобов'язуються здійснювати прозорий нагляд за інституцією та забезпечують її незалежність і плюралістичне управління,

   то інституція збереже легітимність, уникне політизації та слугуватиме стійким механізмом координації демократичних зусиль в суперечливому глобальному інформаційному середовищі.

7. Насамкінець, **якщо** демократичні країни узгодять фінансування та стратегічну підтримку незалежних медіа та організацій громадянського суспільства у вразливих регіонах, а демократичні уряди нададуть необхідну дипломатичну підтримку,

   то спеціалізовані національні інституції зможуть краще сприяти такому: (а) більш ефективній розбудові спроможності та підтримці захисників доброчесності інформації на передньому краї, які підтримують демократичні цінності та принципи; (б) підтримці місцевих або національних виборчих органів та інших зацікавлених сторін для підвищення готовності до виборів шляхом моніторингу, планування сценаріїв та швидкого реагування; (в) узгодженню рекомендацій для урядів щодо спільних норм, стандартів та можливих варіантів державної політики, в основі яких містяться демократичні цінності та широка довіра суспільства.

Розділ 4

ВИСНОВКИ

Різноманітні іноземні і вітчизняні суб'єкти дедалі частіше маніпулюють інформацією і таким чином спотворюють публічний інформаційний простір, у якому відбувається обговорення суспільно важливих питань і в межах якого громадяни формують свою спільну реальність. Ціла низка ініціатив була останнім часом реалізована у демократичних суспільствах для протидії інформаційним загрозам, включаючи FIMI, дезінформацію та інші гібридні форми впливу. Ці ініціативи переважно зосереджувалися на одній загрозі і наразі можемо констатувати, що поки що не вдалося суттєво їх приборкати. Водночас дедалі більша обізнаність суспільства стосовно цих загроз, а також здобутий досвід різних подій у цій сфері підштовхнули уряди і суспільства до визнання того, що демократичні держави мають вжити заходів для підвищення стійкості суспільства до цих шкідливих дій. Це усвідомлення ґрунтується також на розумінні того, що інформаційні екосистеми є складними мережами взаємовідносин, які одночасно відображають основні соціально-політичні та економічні чинники і формують усі процеси прийняття рішень.

Визнаючи необхідність більш комплексного підходу, демократичні країни повинні вирішувати численні нормативні, правові, організаційні та інші питання.

Визнаючи необхідність більш комплексного підходу, демократії повинні опрацювати численні нормативні, правові, організаційні та інші питання. Що робити і як? Складність швидкозмінного інформаційного простору, тонкощі сучасної соціальної структури, інтереси наявних владних інституцій та постійні спроби супротивників вплинути на думку громадськості — це лише деякі з багатьох питань, з якими доводиться мати справу тим, хто приймає рішення. У цьому дискусійному документі стверджується, що одним із варіантів системного вирішення цих проблем є сприяння розвитку відносин, процесів та норм, які забезпечують прогрес як у горизонтальному, так і у вертикальному напрямках, як на національному, так і на міжнародному рівні.

З метою розробки концепції та початкових планів щодо створення нової державної установи, яка б виступала координаційним центром для узгоджених зусиль, можна було б створити невелику робочу групу, до

складу якої увійшли б національні та міжнародні експерти. За допомогою інтерв'ю з видатними громадськими діячами та представниками уряду і громадянського суспільства, а також досліджень і аналізу, ця робоча група могла б розробити мандат, описати функції та організаційну структуру спеціалізованої установи з протидії дезінформації, а також інші ключові елементи, що дасть змогу провести більш цілеспрямоване обговорення та аналіз.

Створюючи нову установу, яка буде зосереджуватися на системних викликах у сфері інформації, демократичні країни зможуть спиратися на здобутий досвід, відкриваючи при цьому нові можливості для взаємодії та підвищення стійкості суспільств. Щоб протистояти дедалі більшій глобальній конкуренції, новим загрозам та викликам, демократичні суспільства мають зміцнювати довіру та співпрацю як всередині своїх кордонів, так і у взаємодії з зовнішніми партнерами. Щоб мати можливість лідирувати у світовій спільноті, демократичні суспільства мають запропонувати потужну візію, якої слід дотримуватися, — як, власне, забезпечити цілісність глобального інформаційного середовища, адже це є важливим суспільним надбанням. Своєю чергою, це прокладе шлях до забезпечення як національних інтересів, так і прав та свобод людини.

Посилання

Adam, I., Lai, S., Nelson, A., Wanless, A. and Yadav, K., 'Emergency Management and Information Integrity: A Framework for Crisis Response', Working Paper, Carnegie Endowment for International Peace [Адам І., Лай С., Нельсон А., Ванлесс А. та Ядав К. Управління надзвичайними ситуаціями та цілісність інформації: основа для реагування на кризи. Робочий документ Фонд Карнегі за міжнародний мир], 9 листопада 2023 року, <https://carnegieendowment.org/research/2023/11/emergency-management-and-information-integrity-a-framework-for-crisis-response?lang=en>, дата перегляду: 9 жовтня 2025 року.

Alkema, B., 'Policy proposal for the creation of a European Resilience Council', SAUFEX [Алкема Б. Пропозиція щодо створення Європейської ради з питань стійкості. SAUFEX], 23 січня 2025 року, <https://saufex.eu/post/26-Policy-proposal-for-the-creation-of-a-European-Resilience-Council>, дата перегляду: 9 жовтня 2025 року.

Asia–Pacific Development, Diplomacy & Defence Dialogue (AP4D), *What Does It Look Like for Australia to Use All Tools of Statecraft in the Information Environment*, Options Paper [Азіатсько-Тихоокеанський діалог *з питань* розвитку, дипломатії та оборони (AP4D), *Як виглядає використання всіх інструментів державного управління в Австралії в інформаційному середовищі*. Документ з варіантами рішень] (Канберра: AP4D, 2024), <https://asiapacific4d.com/idea/information-environment>, дата перегляду: 9 жовтня 2025 року.

Asplund, E. and Casentini, S., 'Protecting elections in the face of online malign threats', [Асплунд Е., Касентіні С. Захист виборів від загроз маніпулятивного дискурсу в Інтернеті. Міжнародний інститут демократії та сприяння виборам (International IDEA)], 9 січня 2024 року, <https://www.idea.int/news/protecting-elections-face-online-malign-threats>, дата перегляду: 9 жовтня 2025 року.

Bentzen, N., 'Information Integrity Online and the European Democracy Shield', European Parliamentary Research Service [Бентцен Н. Цілісність інформації в Інтернеті та Європейський щит демократії. Дослідницька служба Європейського Парламенту], 10 грудня 2024 року, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)767153>, дата перегляду: 9 жовтня 2025 року.

Berndtsson, J., 'Total defence for the 21st century?', Australian Institute of International Affairs [Берндтссон Дж. Тотальна оборона у 21 столітті? Австралійський інститут міжнародних відносин], 5 квітня 2024 року, <https://www.internationalaffairs.org.au/australianoutlook/total-defence-for-the-21st-century>, дата перегляду: 9 жовтня 2025 року.

Bicu, I., 'The information environment around elections', [n.d.] [Біку І. Інформаційне середовище навколо виборів. Міжнародний інститут демократії та сприяння виборам (International IDEA) [без дати], <https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections>, дата перегляду: 9 жовтня 2025 року.

Bradshaw, S., 'Influence operations and disinformation on social media', Centre for International Governance Innovation [Бредшоу С. Операції впливу та дезінформація в соціальних мережах. Центр інновацій у сфері міжнародного управління], 23 листопада 2020 року, <https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media>, дата перегляду: 9 жовтня 2025 року.

Canada, Government of, Government of the United States and Government of the United Kingdom, 'Joint statement by Canada, United States and United Kingdom on foreign information manipulation', Global Affairs Canada [Уряд Канади, Уряд Сполучених Штатів та Уряд Сполученого Королівства. Спільна заява Канади, Сполучених Штатів та Сполученого Королівства щодо маніпулювання інформацією з-за кордону. Global Affairs Canada], 16 лютого 2024 року, <https://www.canada.ca/en/global-affairs/news/2024/02/joint-statement-by-canada-united-states-and-united-kingdom-on-foreign-information-manipulation.html>, дата перегляду: 9 жовтня 2025 року.

Canada, Government of, 'Global declaration on information integrity online' [Уряд Канади. Глобальна декларація про цілісність інформації в Інтернеті], 29 жовтня 2024 року, <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/declaration_information_integrity-integrite.aspx?lang=eng>, дата перегляду: 9 жовтня 2025 року.

Charon, P. and Jeangène Vilmer, J.-B., *Chinese Influence Operations: A Machiavellian Moment* (Paris: IRSEM, 2021) [Чарон П., Жанжен Вільмер Ж.-Б. *Операції китайського впливу: макіавеллістський момент* (Париж: IRSEM, 2021)], <https://www.irsem.fr/report.html>, дата перегляду: 9 жовтня 2025 року.

Châtelet, V. and Lesplingart, A., 'Russia's Pravda network in numbers: Introducing the Pravda Dashboard' [Шателе В., Лесплінгарт А. Мережа «Правда» Росії в цифрах: представлення інформаційної панелі «Правда»], DFRLab, 18 квітня 2025 року, <https://dfrlab.org/2025/04/18/introducing-the-pravda-dashboard>, дата перегляду: 9 жовтня 2025 року.

Chenrose, A. and Rizzuto, M., 'The evolving role of AI-generated media in shaping disinformation campaigns' [Ченроуз А., Різзуто М. Еволюція ролі ЗМІ, що генеруються штучним інтелектом, у розробці кампаній з дезінформації. DFRLab], 1 травня 2025 року, <https://dfrlab.org/2025/05/01/the-evolving-role-of-ai-generated-media-in-shaping-disinformation-campaigns>, дата перегляду: 9 жовтня 2025 року.

Council of Europe, 'Digital citizenship education', [n.d.] [Рада Європи. Освіта в галузі цифрового громадянства [без дати]], <https://www.coe.int/en/web/education/digital-citizenship-education>, дата перегляду: 9 жовтня 2025 року.

Council of Europe Committee on Political Affairs and Democracy, 'Fostering societal resilience to counter foreign interference operations' [Комітет Ради Європи з політичних питань і демократії. Сприяння стійкості суспільства для протидії операціям іноземного втручання], 5 березня 2025 року, <https://pace.coe.int/en/news/9790/fostering-societal-resilience-to-counter-foreign-interference-operations>, дата перегляду: 9 жовтня 2025 року.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 'Hybrid threats as a concept', [n.d.] [Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE). Гібридні загрози як концепція [без дати]], <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon>, дата перегляду: 9 жовтня 2025 року.

European Commission, 'Strategic communication and countering foreign information manipulation and interference', [n.d.] [Європейська комісія. Стратегічна комунікація та протидія іноземній маніпуляції інформацією та втручанню [без дати]], <https://commission.europa.eu/topics/countering-information-manipulation_en>, дата перегляду: 9 жовтня 2025 року.

European External Action Service (EEAS), '1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence', [Європейська служба зовнішніх справ (ЄСЗС). 1-й звіт ЄСЗС про загрози маніпулювання інформацією та втручання з боку іноземних держав: на шляху до створення системи мережевої оборони], 7 лютого 2023 року, <https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en>, дата перегляду: 9 жовтня 2025 року.

European External Action Service (EEAS), '3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations', [Європейська служба зовнішніх справ (ЄСЗС). 3-й звіт Європейської служби зовнішніх справ про маніпулювання іноземною інформацією та загрози втручання: аналіз архітектури операцій FIMI], 19 березня 2025 року, <https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en>, дата перегляду: 9 жовтня 2025 року.

EUvsDisinfo, 'In Russia's FIMI laboratory: Test case, Moldova' [EUvsDisinfo. У російській лабораторії FIMI: тестовий кейс, Молдова], 22 квітня 2025 року, <https://euvsdisinfo.eu/in-russias-fimi-laboratory-test-case-moldova>, дата перегляду: 9 жовтня 2025 року.

France, Government of, Decree No. 2021-922 of 13 July 2021 establishing a service with national jurisdiction [Уряд Франції. Декрет № 2021-922 від 13 липня 2021 року про створення служби, що має загальнонаціональні повноваження] <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361>, дата перегляду: 9 жовтня 2025 року.

Foreign Information Manipulation and Interference – Information Sharing and Analysis Centre (FIMI–ISAC), 'Collective Findings I: Elections' [Маніпулювання інформацією та втручання іноземних держав — Центр обміну та аналізу інформації (FIMI–ISAC), «Колективні висновки I: Вибори»], жовтень 2024 року, <https://www.disinformationindex.org/research/2024-10-21-fimi-isac-collective-findings-report-on-2024-european-elections>, дата перегляду: 9 жовтня 2025 року.

Giannopoulos, G., Smith, H. and Theocharidou, M., *The Landscape of Hybrid Threats: A Conceptual Model* (Luxembourg: Publications Office of the European Union, 2021) [Джаннопулос Г., Сміт Г., Теохаріду М. *Ландшафт гібридних загроз: концептуальна модель* (Люксембург: Видавничий офіс Європейського Союзу, 2021 рік)], <https://doi.org/10.2760/44985>

Heinmaa, T., *Winning Elections the Right Way: Online Political Advertising Rules in Europe and Selected Countries Globally* [Heinmaa T. *Перемагати на виборах правильним шляхом: правила політичної реклами онлайн в Європі та окремих країнах світу.* Стокгольм: Міжнародний інститут демократії та сприяння виборам (International IDEA), 2023 рік], <https://doi.org/10.31752/idea.2023.77>.

Johnson, D. B., 'U.S. election official: "Whack-a-mole" strategies less effective to combat disinfo', CyberScoop [Джонсон Д. Б. Офіційний представник виборчої комісії США: стратегії «вдар крота» менш ефективні в боротьбі з дезінформацією. CyberScoop], 18 червня 2024 року, <https://cyberscoop.com/u-s-election-officialwhack-a-mole-strategies-less-effective-to-combat-disinfo>, дата перегляду: 9 жовтня 2025 року.

Keller, C. I., Freihse, C. and Berger, C., *State Actions against Disinformation: Towards a Healthy Public Sphere* (Gütersloh: Bertelsmann Stiftung, 2024) [Келлер К. І., Фрайзе К., Бергер К. *Державні заходи проти дезінформації: на шляху до*

здорової публічної сфери (Гютерсло: Bertelsmann Stiftung, 2024)], <https://doi.org/10.11586/2024064>

McPherson, P., 'Fake accounts drove praise of Duterte and now target Philippine election', Reuters [Макферсон П. Фейкові акаунти вихваляли Дутерте, а тепер спрямували своє вістря на вибори на Філіппінах. Reuters], 11 квітня 2025 року, <https://www.reuters.com/world/asia-pacific/fake-accounts-drove-praise-duterte-now-target-philippine-election-2025-04-11>, дата перегляду: 9 жовтня 2025 року.

Nicholson, J., Dortmans, P., Black, M., Kepe, M., Grand-Clement, S., Silfversten, E., Black, J., Ogden, T., Dewaele, L. and Alonso García-Bode, P., 'Defence Mobilisation Planning Comparative Study: An Examination of Overseas Planning', RAND Corporation [Ніколсон Дж., Дортманс П., Блек М., Кепе М., Гранд-Клемент С., Сільфверстен Е., Блек Дж., Огден Т., Деваеле Л., Алонсо Гарсія-Боде П. Порівняльне дослідження планування мобілізації оборони: аналіз планування за кордоном], RAND Corporation, 3 травня 2021 року, <https://www.rand.org/pubs/research_reports/RRA1179-1.html>, дата перегляду: 9 жовтня 2025 року.

North Atlantic Treaty Organization (NATO), 'NATO's approach to counter information threats' [Організація Північноатлантичного договору (НАТО). Підхід НАТО до протидії інформаційним загрозам], 3 лютого 2025 року, <https://www.nato.int/cps/fr/natohq/topics_219728.htm?selectedLocale=en>, дата перегляду: 9 жовтня 2025 року.

Office of the Director of National Intelligence (ODNI), Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA), 'Joint ODNI, FBI, and CISA Statement on Iranian Election Influence Efforts', FBI [Управління директора національної розвідки (ODNI), Федеральне бюро розслідувань (FBI) та Агентство з кібербезпеки та безпеки інфраструктури (CISA). Спільна заява ODNI, FBI та CISA щодо спроб Ірану вплинути на вибори, FBI], 19 серпня 2024 року, <https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts>, дата перегляду: 9 жовтня 2025 року.

Organisation for Economic Co-operation and Development (OECD), 'Mis- and disinformation', [n.d.a] [Організація економічного співробітництва та розвитку (ОЕСР). Хибна інформація та дезінформація [без дати]], <https://www.oecd.org/en/topics/sub-issues/disinformation-and-misinformation.html>, дата перегляду: 9 жовтня 2025 року.

Organisation for Economic Co-operation and Development (OECD), 'Open government and citizen participation', [n.d.b] [Організація економічного співробітництва та розвитку (ОЕСР). Відкритий уряд та участь громадян [без дати]], <https://www.oecd.org/en/topics/sub-issues/open-government-and-citizen-participation.html>, дата перегляду: 9 жовтня 2025 року.

Organisation for Economic Co-operation and Development (OECD), *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave* (Paris: OECD Publishing, 2020) [Організація економічного співробітництва та розвитку (ОЕСР). *Інноваційна участь громадян та нові демократичні інституції: ловлячи хвилю деліберації*] (Париж: Видавництво ОЕСР, 2020), <https://doi.org/10.1787/339306da-en>

Organisation for Economic Co-operation and Development (OECD), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action* (Paris: OECD, 2022) [Організація економічного співробітництва та розвитку (ОЕСР), *Будування довіри та зміцнення демократії: підготовка ґрунту для дій уряду*] (Париж: ОЕСР, 2022), <https://doi.org/10.1787/76972a4a-en>

Organisation for Economic Co-operation and Development (OECD), '2024 Global Forum on Building Trust and Reinforcing Democracy: Breaking New Ground for the Future of Democracy', Key Issues Paper, 2024a [Організація економічного співробітництва та розвитку (ОЕСР). Глобальний форум 2024 року з питань зміцнення довіри та демократії: Нові горизонти для майбутнього демократії. Документ з ключових питань, 2024a], <https://www.oecd.org/content/dam/oecd/en/about/programmes/reinforcing-democracy-initiative/2024-OECD-Global-Forum-Key-Issues-Paper.pdf>, дата перегляду: 9 жовтня 2025 року.

Organisation for Economic Co-operation and Development (OECD), 'Recommendation of the Council on Information Integrity', OECD/LEGAL/0505 [Організація економічного співробітництва та розвитку (ОЕСР). Рекомендація Ради щодо цілісності інформації, OECD/LEGAL/0505], 17 грудня 2024b, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505>, дата перегляду: 9 жовтня 2025 року.

Palmertz, B., Weissmann, M., Nilsson, N. and Engvall, J., *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference* (Lund University Psychological Defence Research Institute, 2024) [Палмертц Б., Вайсманн М., Нільссон Н, Енгвалл Дж. *Формування стійкості та психологічного захисту*: *аналітична основа для протидії гібридним загрозам, іноземному впливу та втручанню* (Інститут досліджень психологічного захисту Лундського університету, 2024 рік)], <https://mpf.se/psychological-defence-agency/publications/archive/2024-03-25-building-resilience-and-psychological-defence---an-analytical-framework-for-countering-hybrid---threats-and-foreign-influence-and-interference>, дата перегляду: 9 жовтня 2025 року.

Parliament of the Republic of Moldova, Decision No. 416 on the concept of strategic communication and countering disinformation, acts of information manipulation and foreign interference for the years 2024-2028, HP416/2023 [Парламент Республіки Молдова, Рішення № 416 стосовно концепції стратегічної комунікації та протидії дезінформації, актам маніпулювання інформацією та іноземному втручанню на 2024–2028 роки, HP416/2023], 22 грудня 2023 року, <https://www.legis.md/cautare/getResults?doc_id=141254&lang=ro>, дата перегляду: 9 жовтня 2025 року.

Polish Ministry of Foreign Affairs, 'Council for Resilience, joint initiative by MFA and civil society organisations against international disinformation, begins operation' [Міністерство закордонних справ Польщі. Рада з питань стійкості, спільна ініціатива МЗС та організацій громадянського суспільства проти міжнародної дезінформації розпочинає свою діяльність], 3 квітня 2025 року, <https://www.gov.pl/web/diplomacy/council-for-resilience-joint-initiative-by-mfa-and-civil-society-organisations-against-international-disinformation-begins-operation>, дата перегляду: 9 жовтня 2025 року.

Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM), 'Manipulation d'algorithmes et instrumentalisation d'influenceurs: enseignements de l'élection présidentielle en Roumanie & risques pour la France' [Служба спостереження та захисту від іноземного втручання у цифровій сфері (VIGINUM). Маніпулювання алгоритмами та інструменталізація інфлюенсерів: досвід президентських виборів у Румунії та ризики для Франції], лютий 2025 року, <https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf>, дата перегляду: 9 жовтня 2025 року.

Service de vigilance et de protection contre les ingérences numériques étrangères, VIGINUM [Служба спостереження та захисту від іноземного втручання у цифровій сфері] [без дати]], <https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques>, дата перегляду: 9 жовтня 2025 року.

Sessa, M. G., Serrano, R. M., Romero-Vicente, A., McNamee, J., Gentil, I. and Alaphilippe, A., 'Countering Disinformation: Issues and Solutions for EU Decisionmakers', EU Disinfo Lab [Сесса М. Г., Серрано Р. М., Ромеро-Вісенте А., МакНамі Дж., Жантіль І., Алафіліп А. Протидія дезінформації: проблеми та рішення для осіб, що приймають рішення в ЄС. EU Disinfo Lab], 4 жовтня 2024 року, <https://www.disinfo.eu/countering-disinformation-issues-and-solutions>, дата перегляду: 9 жовтня 2025 року.

Sicurella, F. G. and Morača, T., *Analysing Enablers and Incentives of Election-Related Foreign Information Manipulation and Interference: A Global Methodology* [Сікурелла Ф.Г., Морача Т. *Аналіз факторів та стимулів маніпулювання інформацією та втручання іноземних держав у виборчий процес: глобальна методологія* (Стокгольм: Міжнародний інститут демократії та сприяння виборам (International IDEA), 2025), <https://doi.org/10.31752/idea.2025.48>

Spain, Government of, Order PCM/1030/2020 of 30 October, publishing the Procedure for Action against Disinformation [Уряд Іспанії, Наказ PCM/1030/2020 від 30 жовтня стосовно Процедури дій проти дезінформації], <https://www.boe.es/eli/es/o/2020/10/30/pcm1030>, доступ 9 жовтня 2025 року.

Spain, Government of, «Presentación del libro: «Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil» [Уряд Іспанії. Презентація книги: *Боротьба з кампаніями дезінформації у сфері національної безпеки: пропозиції громадянського суспільства*], 27 вересня 2022 року, <https://www.dsn.gob.es/en/node/18297>, дата перегляду: 9 жовтня 2025 року.

Spain, Government of, 'Order PJC/248/2025, of March 13, approving the procedure for developing the National Strategy against Disinformation Campaigns' [Уряд Іспанії. Наказ PJC/248/2025 від 13 березня, яким затверджується процедура розробки Національної стратегії протидії кампаніям з дезінформації], 13 березня 2025a, <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151>, дата перегляду: 9 жовтня 2025 року.

Spain, Government of, 'Work by the Forum against Disinformation Campaigns: 2024 Initiatives', July 2025b [Уряд Іспанії. Робота Форуму проти дезінформаційних кампаній: ініціативи 2024 року], липень 2025b, <https://www.dsn.gob.es/sites/default/files/2025-07/Disinformation%20Campaigns%202024%20Initiatives.pdf>, дата перегляду: 9 жовтня 2025 року.

Swedish Psychological Defence Agency (SPDA) [n.d.] [Шведське агентство психологічного захисту (SPDA), [без дати]], <https://mpf.se/psychological-defence-agency>, дата перегляду: 9 жовтня 2025 року.

Tofvesson, M. and Kozłowski, A., 'Combatting disinformation by state agencies: The case of the Swedish Psychological Defence Agency', *New Eastern Europe* [Тофвессон М., Козловскі А. Боротьба державних установ з дезінформацією: Приклад Шведського агентства психологічного захисту, *New Eastern Europe*], 7 травня 2024 року, <https://neweasterneurope.eu/2024/05/07/combatting-disinformation-by-state-agencies-the-case-of-the-swedish-psychological-defence-agency>, дата перегляду: 9 жовтня 2025 року.

United Nations, 'United Nations Global Principles for Information Integrity', [n.d.], [Організація Об'єднаних Націй. Глобальні принципи Організації Об'єднаних Націй щодо цілісності інформації [без дати]], <https://www.un.org/en/information-integrity/global-principles>, дата перегляду: 9 жовтня 2025 року.

United Nations Development Programme (UNDP) Policy Centre for Governance, 'Information Integrity for an Open, Inclusive Public Sphere and Informed Civic Engagement', [n.d.] [Програма розвитку Організації Об'єднаних Націй (ПРООН) Центр політики управління. Цілісність інформації для відкритої, інклюзивної суспільної сфери та поінформованої громадянської активності [без дати]], <https://www.undp.org/information-integrity>, дата перегляду: 9 жовтня 2025 року.

United States Department of State, 'Democratic roadmap: Building civic resilience to the global digital information manipulation challenge', [n.d.] [Державний департамент США. Демократична дорожня карта: формування громадянської стійкості до глобального виклику маніпулювання цифровою інформацією [без дати]], <https://2021-2025.state.gov/roadmap-info-integrity>, дата перегляду: 9 жовтня 2025 року.

B Van der Staak, S. and Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration* [Б Ван дер Стаак С., Вольф П. *Кібербезпека під час виборів: моделі міжвідомчої співпраці* (Стокгольм: Міжнародний інститут демократії та сприяння виборам (International IDEA), 2019)], <https://doi.org/10.31752/idea.2019.23>

Wanless, A. and Berk, M., 'The audience is the amplifier: Participatory propaganda', in P. Baines, N. O'Shaughnessy and N. Snow (eds), *The SAGE Handbook of Propaganda* [Ванлесс А.,Берк М. Аудиторія є підсилювачем: пропаганда на основі широкої громадської участі, у праці П. Бейнс, Н. О'Шонесі та Н. Сноу (ред.). *Посібник SAGE з пропаганди* (Лондон: Sage, 2019)], <https://doi.org/10.4135/9781526477170.n7>

Wanless, A., Lai, S. and Hicks, J., 'Assessing National Information Ecosystems', Carnegie Endowment for International Peace [Ванлесс А., Лай С., Хікс Дж. Оцінка національних інформаційних екосистем. Фонд Карнегі за міжнародний мир], 11 лютого 2025 року, <https://carnegieendowment.org/research/2025/02/assessing-national-information-ecosystems?lang=en>, дата перегляду: 9 жовтня 2025 року.

Zimonjic, P., '5 things we learned from the final report on foreign interference' [Зимоніч П. 5 речей, які ми дізналися з кінцевого звіту про іноземне втручання], CBC News, 28 січня 2025 року, <https://www.cbc.ca/news/politics/final-report-public-inquiry-foregin-interference-1.7443597>, дата перегляду: 9 жовтня 2025 року.

Про автора

Майкл Берк — канадський радник зі стратегічних питань, що обіймав посади в уряді. Спеціалізується на питаннях доброчесності інформації, безпеки та управління інформацією. З 2021 по 2024 рік пан Берк працював координатором Механізму швидкого реагування країн Великої сімки (G7) у Міністерстві закордонних справ Канади. Його обов'язки на цій посаді передбачали координацію багатосторонніх зусиль з протидії іноземному втручанню та дезінформації в демократичних країнах. Майкл Берк є співавтором публікацій, присвячених пропаганді та інформаційним операціям, що базуються на участі громадськості. Пан Берк робить істотний внесок у політичний дискурс стосовно питань цифрових загроз та стійкості суспільства. Майкл Берк продовжує надавати консультації з питань інноваційного розвитку у суспільно-політичних відносинах, діагностичного моделювання та співпраці між різними суб'єктами з метою зміцнення національних інформаційних екосистем.

Про Міжнародний інститут демократії та сприяння виборам (International IDEA)

Міжнародний інститут демократії та сприяння виборам (International IDEA) — це міжурядова організація, заснована в 1995 році, до складу якої входять 35 держав-членів. Її завданням є підтримка сталого розвитку демократії в усьому світі.

ЩО МИ РОБИМО

Ми проводимо дослідження у сфері виборів, парламентаризму, конституційного права, цифрової трансформації, кліматичних змін, інклюзії та політичного представництва, керуючись Цілями сталого розвитку ООН. Рекомендації, розроблені в результаті наших досліджень, можуть бути покладені в основу національної або регіональної політики. Ми проводимо оцінку ефективності демократичних систем у різних країнах світу за допомогою унікальних індексів Global State of Democracy Indices та Democracy Tracker.

Ми надаємо допомогу в розбудові спроможності та експертні консультації для демократичних інститутів, до яких належать уряди, парламенти, органи адміністрування виборів та громадянське суспільство. Ми розробляємо інструменти та публікуємо бази даних, книги та посібники різними мовами з широкого спектру тем – від явки виборців до гендерних квот.

Ми сприяємо діалогу та обміну досвідом між державними та недержавними інститутами. Ми виступаємо на захист демократії та її поширення у всьому світі.

ДЕ МИ ПРАЦЮЄМО

Наша штаб-квартира знаходиться в Стокгольмі, а регіональні та країнові офіси – в країнах Африки і Західної Азії, Азії та Тихоокеанського регіону, Європи, Латинської Америки і Карибського басейну. Міжнародний інститут демократії та сприяння виборам є постійним спостерігачем в Організації Об'єднаних Націй та акредитований в інституціях Європейського Союзу.

НАШІ ПУБЛІКАЦІЇ ТА БАЗИ ДАНИХ

На нашому вебсайті розміщено каталог із понад 1000 публікацій та понад 25 баз даних. Більшість наших публікацій можна завантажити безкоштовно.

<https://www.idea.int>

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

В епоху дедалі більшого поширення маніпулювання інформацією та дезінформації демократичні суспільства стикаються із щораз складнішими загрозами. Кампанії маніпулювання суспільним дискурсом, що проводяться як державними, так і недержавними суб'єктами, використовують уразливість національних інформаційних екосистем, а це, своєю чергою, розхитує суспільну довіру, поглиблює поляризацію та руйнує впевненість у демократичних процесах. Для протидії цим загрозам було започатковано низку ініціатив, але вони здебільшого залишаються фрагментарними та нерівномірними. Труднощі полягають не лише у виявленні та протидії дезінформації, а й у подоланні глибших системних явищ, через які демократичні суспільства стають вразливими до маніпуляцій.

Головна ідея цього документу для обговорення полягає в тому, що демократії повинні запровадити більш системний, загальносуспільний підхід до реагування на загрози в інформаційній екосистемі та відійти від ситуативних і розрізнених методів. У ньому міститься заклик до створення спеціалізованих національних інституцій з метою захисту доброчесності інформації. Діяльність таких інституцій полягала би у сприянні виробленню колективного розуміння загроз в інформаційній екосистемі, підтримці міжгалузевої співпраці та формуванні суспільної резистентності у довгостроковому вимірі. На основі інформації з відкритих джерел, інтерв'ю з експертами та порівняльного аналізу в документі окреслено основні елементи, які суспільно-політичні діячі і всі зацікавлені сторони можуть використовувати для розроблення державної політики у цій сфері.

ISBN: 978-91-8137-110-9 (PDF -файл)