



Інститут
національної
стійкості та безпеки

Стойка Європа.

Протидія шантажу та
маніпуляціям в агресивних
інформаційних потоках

Спеціальна редакція звіту



AI DEFENCE
SUMMIT
2026

2 лютого 2026
inrs.net.ua



Зображення команди Інституту національної стійкості та безпеки (зліва–направо): Рена Марутян, директорка; Дмитро Ланде, радник з питань інформаційної безпеки та ШІ; Елліна Шнурко-Табакова, директорка зі стратегічного розвитку та аналітики.

Аналітика, що пояснює. Моделі, що передбачають. Рішення, що працюють

Сучасні реалії агресії Росії проти України сприяють фундаментальним зсувам у сприйнятті сучасної війни західними демократіями, членами ЄС та НАТО. Західні політики та посадовці оборонного сектору офіційно визнали: межа між миром та війною остаточно розмита, а кібератаки, диверсії та дезінформація тепер розглядаються як пряма підготовка до військового зіткнення.

Досвід, що набула Україна в протидії гібридним впливам аж ні як не менший, ніж досвід перемог та стримування фронтів. Інститут національної стійкості та безпеки об'єднує фахівців та науковців, які з 2014 року працюють у проектах протидії гібридним впливам РФ. Поєднання експертизи гуманітарних та математичних наук створює унікальне середовище імплементації інноваційних розроблень у державні системи підтримки прийняття рішень. Синергія поєднання гуманітарної та технічної складових дозволяє Інституту діяти комплексно – одночасно працювати з технологіями й зі смислами, з даними й з людьми. Саме ця міждисциплінарність робить Інститут інтелектуальним майданчиком співпраці між державою, академічною спільнотою, бізнесом, медіа та громадянським суспільством.

Основна мета Інституту – створити екосистему, що об'єднує дослідників, аналітиків, практиків та науковців у сфері міжнародної та національної безпеки, зокрема для зменшення наслідків гібридних загроз зі сторони РФ та її геополітичних союзників.

У грудні 2025 року у Брюсселі відбувся форум «Стійка Європа: протидія російській пропаганді та дезінформації», який зібрав понад 100 учасників з більш ніж 20 країн – представників державних інституцій, експертної спільноти, культури, медіа та громадянського суспільства. Під час форуму директорка Інституту національної стійкості та безпеки Рена Марутян представила перший аналітичний продукт Інституту – дослідження «Стратегічна стійкість в умовах гібридного впливу: огляд експертних рекомендацій та стратегічних наслідків», присвячене російським пропагандистським наративам і інструментам впливу в країнах Європейського Союзу. Аналіз інформаційного простору Франції, Іспанії та Бельгії дозволив ідентифікувати найбільш деструктивні меседжі та організації, які системно їх поширюють, і став підґрунтям для подальшої професійної дискусії з європейськими партнерами.

Для саміту AI in Defence Інститут підготував спеціальну редакцію дослідження, що містить додаткові дані щодо ядерного шантажу, який регулярно застосовує РФ, технологічні міфи та додаткові прогнози. Дослідження є сумісним продуктом Аналітичного Центру та Лабораторії ШІ Інституту.

Лабораторія штучного інтелекту є центральним елементом технічного напрямку Інституту і працює над використанням AI-рішень у сфері безпеки та оборони: аналізі великих масивів даних, моніторингу інформаційних загроз, моделюванні сценаріїв та підтримці ухвалення управлінських рішень. Інновації тут розглядаються не як самоціль, а як інструмент посилення інституційної спроможності та стійкості.

Лабораторія штучного інтелекту об'єднує фахівців з багаторічним науковим і практичним досвідом у галузях штучного інтелекту, семантичного аналізу, інформаційної безпеки, права, соціальних комунікацій та сценарного прогнозування. Члени команди Лабораторії є авторами десятків наукових публікацій, у тому числі монографій, і розробниками власних методів та алгоритмів, що успішно застосовуються в складних аналітичних і управлінських задачах.

Ключові напрями реалізованих проєктів і компетенцій

Інтерактивні семантичні мережі предметних областей

Фахівцями Лабораторії реалізовано проєкти з формування інтерактивних семантичних мереж, що відображають структуру предметних областей і логіку взаємозв'язків між поняттями, подіями, акторами та процесами. Такі мережі використовуються як основа для підготовки аналітичних звітів щодо складних проблем – від безпекових і соціальних до економічних і правових.

Каузальні семантичні мережі та сценарний аналіз

Розроблено власні алгоритми і методики побудови каузальних семантичних мереж із використанням двонаправленого пошуку (від причин до наслідків і навпаки). Це дозволяє:

- моделювати альтернативні сценарії розвитку ситуацій;
- виявляти критичні точки впливу;
- здійснювати ранжування сценаріїв за різними критеріями оптимальності;
- забезпечувати підтримку прийняття рішень у різних галузях – від публічної політики до корпоративного управління.

Аналітика юридичних документів і нормативних масивів

Лабораторія виконує комплексний аналіз юридичних текстів із застосуванням структурованих промптів для великих мовних моделей (ВММ), побудованих на основі власного фреймворку безкодового промпт-програмування. Це дозволяє виявляти:

- ознаки лобювання;
- внутрішню та міждокументну неузгодженість;
- потенційні корупційні ризики;
- приховані зміни смислів і норм.

Виявлення фейків і маніпуляцій

Задачі протидії дезінформації вирішуються на основі аналізу достовірності зв'язків у семантичних мережах. Такий підхід дозволяє переходити від поверхневої перевірки фактів до структурного аналізу смислових викривлень і маніпулятивних конструкцій.

Генерація цільових комунікацій і рекламних текстів

На основі сформованих і експертно скоригованих семантичних мереж здійснюється реінжиніринг змісту з подальшою генерацією текстів, орієнтованих на первинні категорії користувачів. Це забезпечує смислову цілісність, релевантність і керованість повідомлень.

Виявлення зв'язків між персонами, компаніями та подіями

Лабораторія реалізує проекти з екстрагування сутностей із текстових масивів та побудови графів зв'язків із застосуванням RAG-технологій – поєднання інформаційного пошуку та штучного інтелекту. Власні пошукові рішення, зокрема Attack Index, інтегруються у ці процеси для підвищення точності та актуальності результатів.

Методологічна перевага Лабораторії

У своїй роботі Лабораторія спирається на чотири взаємодоповнювальні підходи:

- Семантичний нетворкінг – формування, аналіз і модифікація семантичних та каузальних мереж як пояснювальних моделей реальності.

- «Рій віртуальних експертів» – багаторазове застосування однакових промптів до різних ВММ, з різних ролей і позицій, із подальшим статистичним узагальненням результатів.
- RAG-технології – інтеграція ВММ із власними пошуковими та аналітичними системами для зниження галюцинацій і підвищення актуальності.
- Безкодове промпт-програмування – автоматичне перетворення простих запитів у структуровані промпти з використанням логічних примітивів і формалізованих схем міркування.

Сучасні великі мовні моделі (ВММ) відкрили новий етап автоматизації аналітики, проте мають фундаментальні недоліки, критичні для державного управління, безпеки та відповідальних рішень. Серед них – галюцинації, схильність до поверхневих відповідей («ледащість»), ефект «чорного ящика» та знижена актуальність знань.

Лабораторія системно працює над подоланням цих обмежень, поєднуючи ВММ із формалізованими знаннями, пошуковими технологіями та власними аналітичними фреймворками.

Лабораторія має на меті побудову керованого, пояснюваного та відповідального інтелектуального середовища. Поєднання наукової школи, власних алгоритмів, міждисциплінарної експертизи та практичного досвіду дозволяє реалізовувати проекти будь якого масштабу.

Інститут, та його складові – Аналітичний центр і Лабораторія ШІ готова до співпраці з державними органами, міжнародними організаціями, бізнесом і дослідницькими центрами, пропонуючи рішення, що перетворюють складність на структуру, а дані – на обґрунтовані рішення.

Зміст

Вступ.....	7
1. Контекст	10
1.1. Наративи російського шантажу світової спільноти	10
1.2. Проникнення шкідливого контенту до інформаційного простору ЄС	12
1.3. Проникнення «русского миру» в країни ЄС.....	13
2. Аналітика. Дослідження	15
2.1. Ядерний шантаж.....	15
2.2. Європейський Союз у російському інформаційному просторі	19
2.3. Європейський Союз в англomовному інформаційному просторі російських джерел	23
2.4. «Русский мир» у країнах ЄС	25
2.4.1. Франція	25
2.4.2. Іспанія.....	28
2.4.3. Бельгія	31
3. Рекомендації експертів	34
4. Методологія.....	39
5. Висновки	42
Додаткові джерела	45

Вступ

Російська Федерація системно використовує дезінформацію, пропаганду та маніпулятивні комунікації як ключовий інструмент гібридної війни проти України та Європейського Союзу. Інформаційна агресія Кремля спрямована на підрив довіри до демократичних інституцій, ослаблення єдності ЄС, делегітимацію підтримки України та формування умов для ревізії європейського безпекового порядку.

Це спеціальна версія дослідження «Стратегічна стійкість в умовах гібридного впливу: огляд експертних рекомендацій та стратегічних наслідків» підготовлена для саміту AI in Defence.

Основна частина була представлена під час форуму «Стійка Європа: протидія російській пропаганді та дезінформації» (Брюссель, 17–18 грудня 2025 року). Дослідження поєднує результати медіамоніторингу, аналіз російських пропагандистських нарративів та експертні напрацювання українських фахівців, які мають унікальний практичний досвід протидії інформаційній агресії.

Аналітика демонструє суттєве зростання присутності Європейського Союзу в російському інформаційному просторі – понад 50% за останні роки. Основним драйвером цього зростання є роль ЄС як ключового партнера України у сфері безпеки, санкційної політики та фінансової підтримки. Кремль цілеспрямовано зміщує фокус інформаційних кампаній на дискредитацію Європейського Союзу як головного елемента міжнародної коаліції підтримки України.

У дослідженні продемонстровані особливості технологічного впливу на пропагандистські теми Кремля, здійснено аналіз постійного потоку шантажу світової спільноти ймовірними ядерними ударами, виявлені особливості синхронізації зі світовими подіями та темами допомоги Україні.

Дослідження ідентифікує сталий набір базових російських нарративів, які адаптуються до різних аудиторій і мовних середовищ:

- трактування війни проти України як «проксі-війни НАТО»;
- представлення ЄС і НАТО як слабких, розділених або агресивних акторів;
- підрив суб'єктності України та довіри до партнерів;
- експлуатація економічних, міграційних і ціннісних страхів європейських суспільств.

Окрему увагу приділено аналізу англomовного сегмента російської пропаганди та проникненню ідеології «русского мира» у Франції, Іспанії та Бельгії. Попри відмінності у національних медіаландшафтах, усі три країни демонструють вразливість до окремих груп нарративів – передусім економічних, антинаївських та антиукраїнських. Російські культурні, релігійні та освітні інституції залишаються важливими каналами довгострокового впливу.

Результати фасилітаційної експертної сесії дозволили сформулювати практичні рекомендації, спрямовані на:

- посилення інформаційної та когнітивної стійкості Європейського Союзу;
- удосконалення політик протидії дезінформації;
- розвиток стратегічних комунікацій і публічної дипломатії;
- захист цифрового та інформаційного суверенітету держав-членів ЄС.

Ключовий висновок дослідження полягає в тому, що протидія російській дезінформації потребує **системного, скоординованого та проактивного підходу**. Український досвід протистояння інформаційній війні є критично важливим ресурсом для формування спільної європейської стратегії захисту демократії, безпеки та стійкості.

Ключові слова: Росія, дезінформація, операція під чужим прапором, публічна дипломатія, вироблення політики, європейська стійкість, ядерний шантаж, штучний інтелект.