Рада національної безпеки і оборони України
Центр протидії дезінформації

Видано за сприяння
Консультативної місії ЄС в Україні

# ПОСІБНИК З ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

# ВСТУП

Цей посібник було створено у відповідь на дії противника щодо України в інформаційному просторі. Так, щомісяця Україна піддається впливу тисячі інформаційних, психологічних, кібернетичних та інших видів загроз з боку російської федерації та її союзників-сателітів. Ворог розуміє, що сучасна війна не обмежується землею, морем, повітрям та космосом. Сучасна війна ведеться також в інформаційному та кіберпросторі, основна мета яких – примусити противника виконати твою волю.

Головним інструментом у досягненні цілей гібридної війни є інформаційний вплив. На жаль, перший рік війни продемонстрував, що даний вплив може мати радикально-агресивний характер, при цьому ворог для досягнення своєї мети використовує всі наявні вразливості українського суспільства.

Тому для покращення системи протидії ворожим інформаційним впливам, ознайомлення з її тонкощами, а також демонстрації тактик, технік і процедур противника –

Центр протидії дезінформації зібрав весь наявний досвід у цій сфері та поділив інформацію на наступні розділи:

1. **Техніки та інструменти інформаційного впливу.**

Розділ має на меті продемонструвати, як саме ворог здійснює свою діяльність в інформаційному просторі.

2. **Ворожі ресурси: як їх виявляти та відслідковувати.**

Розділ розкриє інформаційні канали, через які ворог напряму здійснює інформаційний вплив на українське суспільство.

3. **Кейси інформаційного впливу рф (практика Центру).**

Розділ містить приклади ворожого інформаційного впливу, з яким Центр протидії дезінформації успішно впорався з моменту початку широкомасштабного вторгнення.

4. **Рекомендації щодо протидії шкідливому інформаційному впливу та здійснення комунікацій із цільовою аудиторією.**

Розділ описує рекомендації з протидії ворожому інформаційному впливу та ефективного донесення інформації до цільової аудиторії для попередження його наслідків.

5. **Глосарій.**

Розділ перелічує терміни, якими користується Центр протидії дезінформації під час здійснення своєї діяльності.

**Ми сподіваємось, що опанувавши знання, які містяться у цьому посібнику, ви зрозумієте всю важливість протидії ворожому інформаційному впливу, а також збільшите ваш арсенал інструментів і засобів для здійснення успішного спротиву в інформаційному просторі.**

# ТЕХНІКИ ТА ІНСТРУМЕНТИ ІНФОРМАЦІЙНОГО ВПЛИВУ

Інформаційний вплив передбачає потенційно шкідливі форми комунікації, організовані державними суб'єктами або іншими представниками іноземних країн. Вони свідомо втручаються у внутрішні справи країни з метою створення атмосфери недовіри між державою та її громадянами. Різні форми інформаційного впливу можуть застосовуватись окремо, або як частина більшої кампанії інформаційного впливу із використанням широкого спектру технологій. Окрім засобів зв'язку, все — від дипломатичних та економічних санкцій до демонстрації військової сили — може використовуватися для впливу на суспільство.

# Анатомія кампаній інформаційного впливу

### 1. Використання технік впливу

Зв'язки з громадськістю, маркетинг, дипломатія, публіцистика та лобіювання є прикладами загальновизнаних способів впливу на погляди і поведінку людей. Засоби інформаційного впливу імітують зазначені вище форми взаємодії, проте використовують їх деструктивно.

### 2. Зрив публічних обговорень

Іноземні держави використовують інформаційну діяльність з метою впливу на ті сфери та громадські обговорення, від яких вони можуть отримати вигоду. Такий вплив здійснюється і прямо, і опосередковано із застосуванням як засобів відкритої пропаганди, так і прихованого фінансування груп громадянського суспільства. При цьому втручання неуповноважених суб'єктів у державні публічні дебати може змінити уявлення суспільства про ключові погляди та вплинути на прийняття рішень.

### 3. Діяльність у власних інтересах

Засоби інформаційного впливу спрямовуються на досягнення конкретних цілей на користь іноземної держави. Ціллю може бути будь-що — від конкретних рішень до поляризації політичних дискусій.

### 4. Використання вразливостей

Кожне суспільство стикається з певними викликами. Це можуть бути соціальна чи класова напруженість, соціальна нерівність, корупція, безпека чи інші проблеми, що є ключовими для соціального життя. Ворожі країни виявляють та систематично використовують ці вразливі місця для досягнення власних цілей.

# Вразливості в інформаційному просторі

Головною вразливістю для інформаційного впливу є сам процес пізнання людини. Наші думки є результатом певного раціонального процесу, окремих дій або появи нової інформації. Свідки, фахівці у відповідних галузях, представники уряду, яких вважають найкомпетентнішими, та інші особи, які володіють глибокими експертними знаннями, інтерпретують ситуацію з огляду на більш широкий контекст. ЗМІ збирають цю інформацію та розповсюджують її серед різних прошарків суспільства в інтернеті та за його межами. Звичайно, на практиці алгоритм може дещо змінюватися, але загалом — саме так виглядає теорія формування громадської думки в демократичному суспільстві.

# Етапи формування громадської думки

Медійна система

**1. Нова інформація**

Відомості про подію, наукові відкриття, новини ЗМІ, політичні рішення.

**2. Інформація, отримана від експертів, офіційних представників та з надійних джерел**

Така інформація є прокоментованою та проаналізованою свідками, експертами, посадовими особами, які інтерпретують її для широкого загалу.

Громадська думка

**3. Публічна інформація**

Інформація стає загальновідомою. Надалі її обговорюють та тлумачать як віч-на-віч, так і в соціальних мережах.

Когнітивні функції людини

**4. Реципієнт**

Особа безпосередньо отримує інформацію через її належність до певної соціальної групи та за допомогою інформаційних каналів, якими вона користується.

Викривлення інформації або її видозміна через зловмисний шкідливий вплив, на будь-якому з етапів, спотворює здоровий процес формування громадської та персональної думки. Для досягнення цієї мети ворог використовує підставних експертів, підкуплених публічних діячів, фейкові ресурси та «альтернативні» ЗМІ тощо, які в свою чергу керуються наративами.

## Наративи та цільова аудиторія в системі інформаційного впливу рф

Заходи інформаційного впливу передбачають певний сторітелінг. Зображення подій, явищ, організацій, місць чи груп, як правило, формуються таким чином, щоб відповідати заздалегідь створеному уявленню. Історії, що плануються навмисно і використовуються в комунікативній діяльності, називаються стратегічними наративами.

**Визначення задіяних стратегічних наративів та логіки, що за ними стоїть, є важливим кроком у прогнозуванні відповідної реакції. Зазвичай виділяють три ключові види стратегічних наративів:**

1. **Позитивний або конструктивний: «Це правда!»**

Намагається створити альтернативне уявлення про певну проблему. Вписується в, або доповнює та розширює існуючі, добре сформовані стратегічні наративи.

2. **Негативний або руйнівний: «Це брехня!»**

Прагне запобігти появі цілісного і повного уявлення про проблему, або спростувати чи підірвати існуючі в межах цієї теми наративи.

3. **Відволікаючий: «Подивіться сюди!»**

Відволікає увагу від ключових питань за допомогою, наприклад, гумору, мемів, теорій змов чи іншого розважального та легкого для сприйняття контенту. Наповнення залежить від вподобань цільової аудиторії.

Ворог роками успішно використовував ці прості за формою (втім дуже ефективні) техніки побудови наративів, що почало змінюватися лише після початку повномасштабної війни проти України. Така успішність була досягнута якісним аналізом цільової аудиторії.

# Класична схема поділу цільової аудиторії на групи:

**Широка громадськість: найширша вибірка аудиторії.**

Заходи інформаційного впливу, спрямовані на суспільство загалом, через узгодження меседжів із загально розповсюдженими наративами.

**Соціально-демографічний таргетинг: вибірка з конкретних груп.**

Ідентифікуючи аудиторію за допомогою демографічних факторів, таких як вік, дохід, освіта та етнічна приналежність, наративи можуть бути сконструйовані так, щоб впливати на конкретні групи.

**Психографічний таргетинг: індивіди.**

Аналізуючи та категорізуючи великі масиви даних (big data), заходи інформаційного впливу можуть бути націлені на людей з конкретними персональними рисами, політичними вподобаннями, моделями поведінки чи іншими ознаками, що визначають особистість.

У поєднанні з аналізом стратегічних наративів та методів комунікації, аналіз цільової аудиторії допомагає викрити справжню мету інформаційного впливу. Якщо ви розумієте, хто є цільовою аудиторією та чому — буде легше зважено оцінити, що є метою інформаційного впливу. Це в свою чергу допоможе обрати правильні контрзаходи.

# Техніки інформаційного впливу рф

У більшості випадків техніки є нейтральними — ні хорошими, ні поганими. Їх можна використовувати відкритими та прийнятними способами як природну частину демократичного діалогу, так і з хибним та злочинним наміром — як частину кампанії інформаційного впливу. Використання будь-якої з цих технік не завжди є ознакою цілеспрямованого (тим паче ворожого) інформаційного впливу. Чим ворог дуже уміло користується, маскуючи свої техніки впливу під вже згадану природну частину демократичного діалогу суспільства.

Ворог використовує велике різноманіття технік та їх поєднань у побудові своїх кампаній, але тут ми розглянемо лише основні.

# Основні техніки інформаційного впливу рф

**Соціально-когнітивний хакінг**

- Прихована реклама
- Ефект сторони-переможця
- Спіраль мовчання
- Луна-камери та бульбашки фільтрів (інформаційні бульбашки)

**Використання фальшивих особистостей**

- Підставні особи
- Самозванці та шахраї
- Підроблення
- Потьомкінські поселення
- Фейкові медіа

**Зловмисне використання технологій**

- Боти
- Віртуал/сокпапет
- Діпфейк
- Фішинг


## Дезінформація

- Фальсифікація
- Маніпуляція
- Місапропріація
- Сатира та пародія

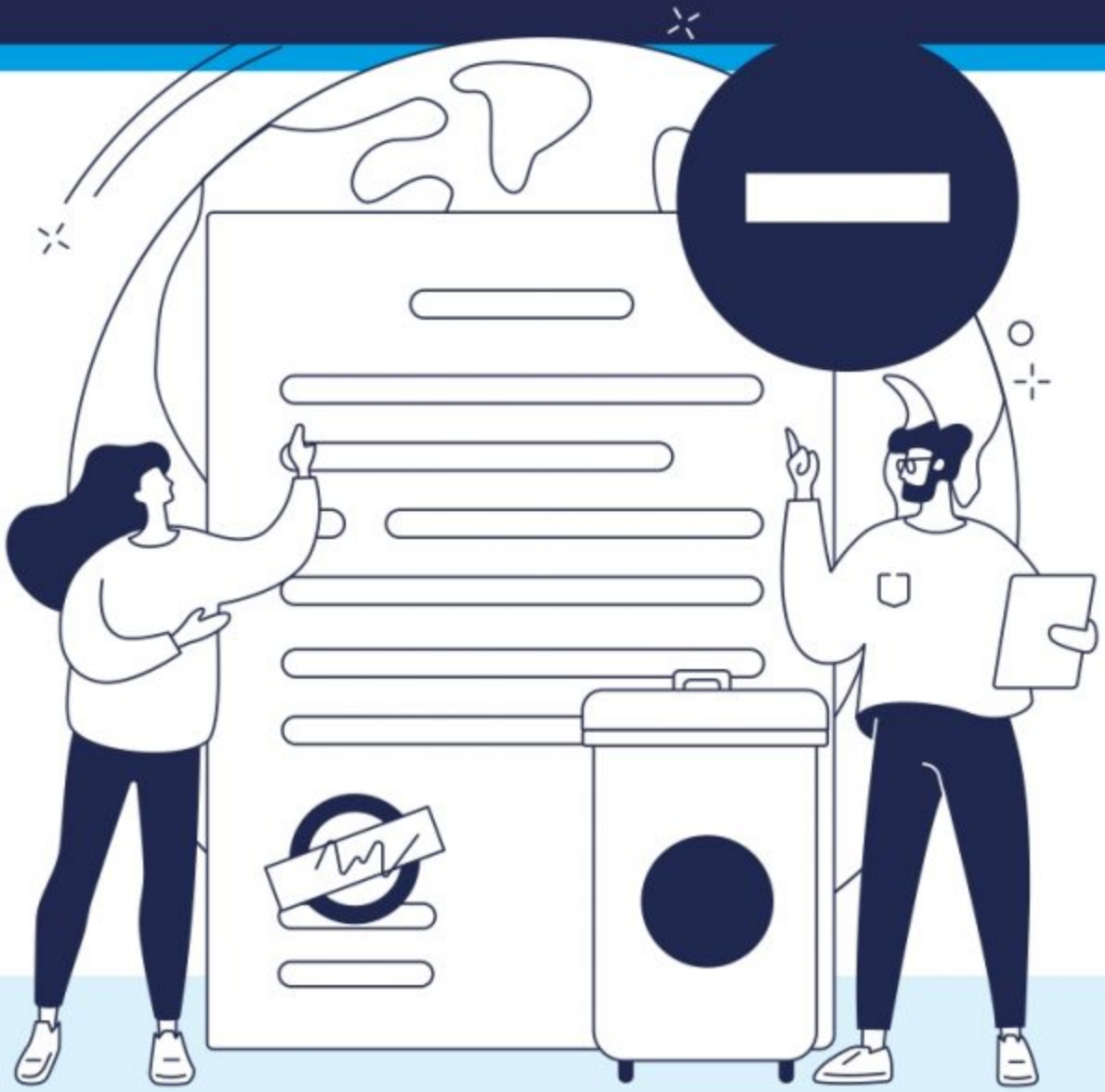
## Маніпулювання риторикою

- Дії, направлені проти конкретних особистостей/Ad hominem
- Якщодоізм/Whataboutism
- Галоп Гіша
- Підміна тез/Strawman
- Перехоплення

## Символічні дії

- Зливи інформації/даних
- Злам
- Публічні демонстрації

# ВОРОЖІ РЕСУРСИ ТА ЯК ЇХ ВІДСТЕЖУВАТИ



# 1. Twitter

Для визначення неавтентичної сторінки у Twitter зазвичай не потрібні інші ресурси або інструменти. У Twitter є достатньо даних для повного аналізу сторінки, такі як:

### 1) Дата створення

За цими даними можна визначити, чи сторінка була створена нещодавно, або завчасно для проведення інформаційної операції.

### 2) Аватар профілю

Зазвичай для ботів та фейкових профілів картинку профілю беруть просто з інтернету. Це надає можливість перевірки картинки через алгоритми розпізнавання зображень, такі як:

1. https://images.google.com/.

2. https://pimeyes.com/en або безкоштовний варіант https://tineye.com/. Ці інструменти створені для розпізнавання обличчя за допомогою парсингу всіх наявних фотографій в інтернеті.

3. У разі вичерпання всіх вищезазначених ресурсів аналізу, через використання VPN можна застосувати https://yandex.ru/images/ для поглибленого пошуку в рунеті.

4. Для аналізу підроблених фотографій рекомендується використовувати https://fotoforensics.com/. Цей інструмент надає можливість через компрес фотографії переглянути, які саме ділянки були змінені або підроблені. Де білий колір означає — непідроблений, а яскраво виражені райдуги означають, що ділянка підроблена.

### 3) Ім'я профілю

У Twitter є два імені профілю, через які можна провести детальніший аналіз. Нікнейм (від англ. nickname) — це ім'я, яке автор може змінювати без значних зусиль. Юзернейм (від англ. username) — це ім'я, яке автор не може змінювати швидко та до нього йде приставка «@» у пошуку. Зазвичай боти та фейкові профілі використовують або найтривіальніші комбінації імен та прізвищ, які є характерними для регіону, або набір символів без конкретного значення. Часто трапляються такі ситуації, коли боти з китайськими чи американськими іменами атакують секції коментарів українських каналів, що відразу можна помітити навіть без додаткових перевірок.

### 4) Активність

Активність профілю дає аналітику велику кількість інформації. Зокрема, це кількість публікацій за певний проміжок часу. Зазвичай велика кількість публікацій в день свідчить про неавтентичність профілю.

### 5) Взаємодія з іншими профілями

Під час аналізу важливо переглянути взаємодію профілю з іншими користувачами. Якщо суб'єкт вашого аналізу активно репостить інформацію інших користувачів, схожих на ботів, або підозрілих ресурсів, найімовірніше профіль оперує в мережі неавтентичної поведінки.

### 6) Мова

Аналізуючи використану мову в публікаціях профілю, можна зрозуміти через правопис чи використовувався машинний переклад під час написання публікації.

### 7) Загальна інформація профілю

У шапці профілю звичайні користувачі іноді залишають корисну інформацію про себе. Неавтентичні профілі в свою чергу або не залишають інформацію, або використовують сфальсифіковану інформацію.

# 2. Медіаресурси

### 1) Посилання URL

Під час інформаційних операцій ворог може створювати безліч фейкових ресурсів, які потрібно ретельно перевіряти. Спочатку важливо перевірити посилання на ресурс, адже ворог може створювати ресурси, які імітують оригінальні.

Важливо зазначити, що треба звертати увагу на протокол посилання. Іноді фейкові медіаресурси використовують протокол HTTP, який є незахищеним. Річ у тому, що дані передаються за HTTP у відкритому вигляді. Це створює ризик розкрити конфіденційну інформацію, якщо хтось перехопить трафік. HTTPs вирішує цю проблему, додаючи в початковий протокол можливість шифрування даних. Також важливо звертати увагу на закінчення посилання, наприклад оригінальний сайт BBC має посилання https://www.bbc.com/, фейкові у свою чергу можуть виглядати так — http://www.bbc.com.co/.

### 2) Заголовок

Головне завдання заголовка — це створити інтерес, щоб користувач зайшов на сторінку ресурсу. Тому, надзвичайно важливо звертати увагу на заголовок і розуміти, які емоції він може у вас викликати.

### 3) Автор

Зазвичай на фейкових медіаресурсах відсутній автор, що також є показником неправдивості інформації. Якщо в сумнівній статті вказаний автор, то його важливо перевірити й подивитись, які ще статті він написав. Автори статей активні в соцмережах, так можна перевірити їх контент за межами статті.

### 4) Джерела

Джерела у статтях надзвичайно важливі, навіть коли статті автентичні. Через них можна зрозуміти, звідки автор черпав інформацію і якими були його наміри. Тому, важливо перевіряти усі зазначені джерела, а за їх відсутності робити правильні висновки.

### 5) Контент

Під час прочитання тексту можна зробити логічний підсумок цілей та ідей, що закладені в статті. Потрібно розуміти та розрізняти інформативну або аргументативну статтю. В якому стилі вона написана, на яких засадах або фактах. Для цього важливо уважно прочитати статтю, навіть декілька разів, і виділити основні тези в ній.

### 6) Картинки

У текстах статті автор може використовувати картинки, які теж потрібно ретельно перевіряти та розуміти, для чого вони там. Автентичність картинки можна перевірити, використовуючи онлайн-ресурси, що зазначені вище.

### 7) Коментарі та активність на сторінці статті

В основному на медіаресурсах є окремий розділ з коментарями. Він також є важливим для аналізу, бо ворог може наповнювати його фейковими коментарями й переписками між користувачами, щоб стаття виглядала правдивішою.

Важливо зазначити, що під час інформаційних операцій ворог може використовувати посилання на фейкові медіаресурси для того, щоб створити видимість популярності статті.

### 8) Інша інформація

Під час аналізу медіаресурсів важливо звертати увагу на інші дані, що вказані в кінці сторінки. Зазвичай компанії залишають потрібну інформацію для користувача, а саме: юридична адреса, посилання на соцмережі, юридичні контактні дані, поштова скринька, реєстрація та авторські права, політика конфіденційності та інше.

### 2) Читати канал

Цей розділ нагадує звичайну стрічку в Telegram, але має декілька додаткових функцій для ґрунтовного аналізу.

- У фільтрі публікацій є функція, яка дозволяє переглянути видалені публікації, а також випадаюче вікно, де можна вибрати рік та місяць публікацій каналу.
- Під окремими публікаціями знизу можна побачити кількість переглядів, пересилань та репостів. Натискаючи на перегляди, можна побачити детальну інформацію щодо переглядів на публікації, а в репостах видно канали і чати, де публікація була поширена.

  Варто зазначити, що даний розділ дозволяє переглядати публікації каналів, які заблоковані в нашому регіоні (наприклад, Рыбарь).

### 3) Цитування

У цьому розділі можна знайти графік з каналами, що найактивніше репостять його і кого канал найчастіше репостить сам. З цього графіку видно можливу мережу каналів, у якій він функціонує та публікує контент.

### 4) Графік публікацій

Цей розділ показує детальний графік публікацій за останній місяць. Це надає можливість впевнитися, що «особистий» канал, який публікує з 9 ранку до 5 вечора, можливо, все-таки ведеться організацією або державною структурою.

### 2) Читати канал

Цей розділ нагадує звичайну стрічку в Telegram, але має декілька додаткових функцій для ґрунтовного аналізу.

- У фільтрі публікацій є функція, яка дозволяє переглянути видалені публікації, а також випадаюче вікно, де можна вибрати рік та місяць публікацій каналу.
- Під окремими публікаціями знизу можна побачити кількість переглядів, пересилань та репостів. Натискаючи на перегляди, можна побачити детальну інформацію щодо переглядів на публікації, а в репостах видно канали і чати, де публікація була поширена.

  Варто зазначити, що даний розділ дозволяє переглядати публікації каналів, які заблоковані в нашому регіоні (наприклад, Рыбарь).

### 3) Цитування

У цьому розділі можна знайти графік з каналами, що найактивніше репостять його і кого канал найчастіше репостить сам. З цього графіку видно можливу мережу каналів, у якій він функціонує та публікує контент.

### 4) Графік публікацій

Цей розділ показує детальний графік публікацій за останній місяць. Це надає можливість впевнитися, що «особистий» канал, який публікує з 9 ранку до 5 вечора, можливо, все-таки ведеться організацією або державною структурою.

# 4. YouTube

Для аналізу неавтентичних відео в YouTube та сторінок, що їх публікують, є достатньо наявних даних на самій платформі. Кількість коментарів, кількість переглядів, кількість підписників. Важливо враховувати, що активність ботів у коментарях можна визначити через доцільність самих коментарів. Коментарі від ботів у більшості випадків не мають змісту або дуже прості за своїм характером.

У аналізі YouTube-каналу має значення перегляд інших розділів на ньому. У розділі «Про канал» знаходяться додаткові посилання каналу, регіон, дата створення, кількість загальних переглядів, контактні дані та опис. Також є розділи «Спільнота» і «Канали», звідки аналітик може отримати додаткову інформацію.

Важливо зазначити, що з появою формату Youtube Shorts значна кількість фейкових відео тепер подається саме у скороченому форматі. Це зумовлено тим, що такі відео легше створювати на смартфоні та, через короткий формат, алгоритм YouTube швидше їх розповсюджує на ширшу аудиторію.

- Для поглибленого аналізу YouTube-каналу існують різноманітні інструменти, але найдоступнішим у своєму використанні є Social blade (https://socialblade.com/). На даному сайті потрібно ввести посилання чи юзернейм каналу, щоб перейти на його сторінку. Тут знаходиться детальніша інформація про канал. У більшості випадків для аналізу потрібен розділ «Детальна статистика». У цьому розділі є інформація про приріст переглядів та підписок каналу в певному проміжку часу. Ці дані дають можливість переглянути нерегулярності у приростi переглядів та активності на каналі.

# 5. Facebook

Для розпізнавання неавтентичної поведінки на сторінках профілів та спільнот у Facebook, необхідно звертати увагу на залученість аудиторії та співвідношення вподобань і підписок. Також важливо звертати увагу на наповненість сторінки. Багато фейкових сторінок у Facebook не мають додаткової інформації, адже неавтентичні профілі не витрачають стільки часу для створення правдоподібної сторінки.

Для ретельної перевірки сторінки у Facebook рекомендовано звертати увагу на наступні розділи:

### 1) Інформація

Напевно, найважливіший розділ для аналізу будь-якої сторінки в соцмережі. Ця частина має важливі дані, які допоможуть у подальшому аналізі сторінки: контактні дані, опис сторінки або профілю, інші соцмережі, кількість підписок, кількість вподобань, відгуки на сторінку, посилання на інші веб-сайти та додаткова інформація про сторінку.

### 2) Розділи Фотографій та Відео

Ці обидва розділи можуть надати додаткову інформацію в аналізі, адже деякі сторінки або спільноти дозволяють своїм користувачам публікувати фотографії на сторінці. У такий спосіб аналітик може ретельно перевірити ці фотографії та знайти потрібні йому зв'язки й інформацію для остаточного висновку.

### 3) Спільноти

На публічних сторінках Facebook іноді можна знайти розділ зі спільнотою. Цей розділ може надати більше інформації про аналізовану мережу, а також розуміння, чи є на цій сторінці бот-активність. Наприклад, спільнота може мати сотні тисяч підписників, але тільки 100-200 реакцій на публікації на сторінці, що свідчить про бот-активність.

### 4) Інше

На сторінках Facebook користувачі або адміністратори самі вирішують, які додаткові розділи матиме їхня сторінка. Тож, важливо під час аналізу ретельно переглядати інші розділи, які можуть містити інформацію про інтереси спільноти та що може обговорюватись на неї. Наприклад, у декількох неавтентичних сторінок Facebook може знаходитись розділ з YouTube.

# 6. Діпфейки

Діпфейк-відео з'явились у 2014 році, на той час вони були доволі прості та легко розпізнавались у порівнянні з оригінальним відео. Проте за короткий проміжок часу технології діпфейків значно розвинулись. Тепер платні інструменти для створення таких відео ледве можна відрізнити від оригіналу.

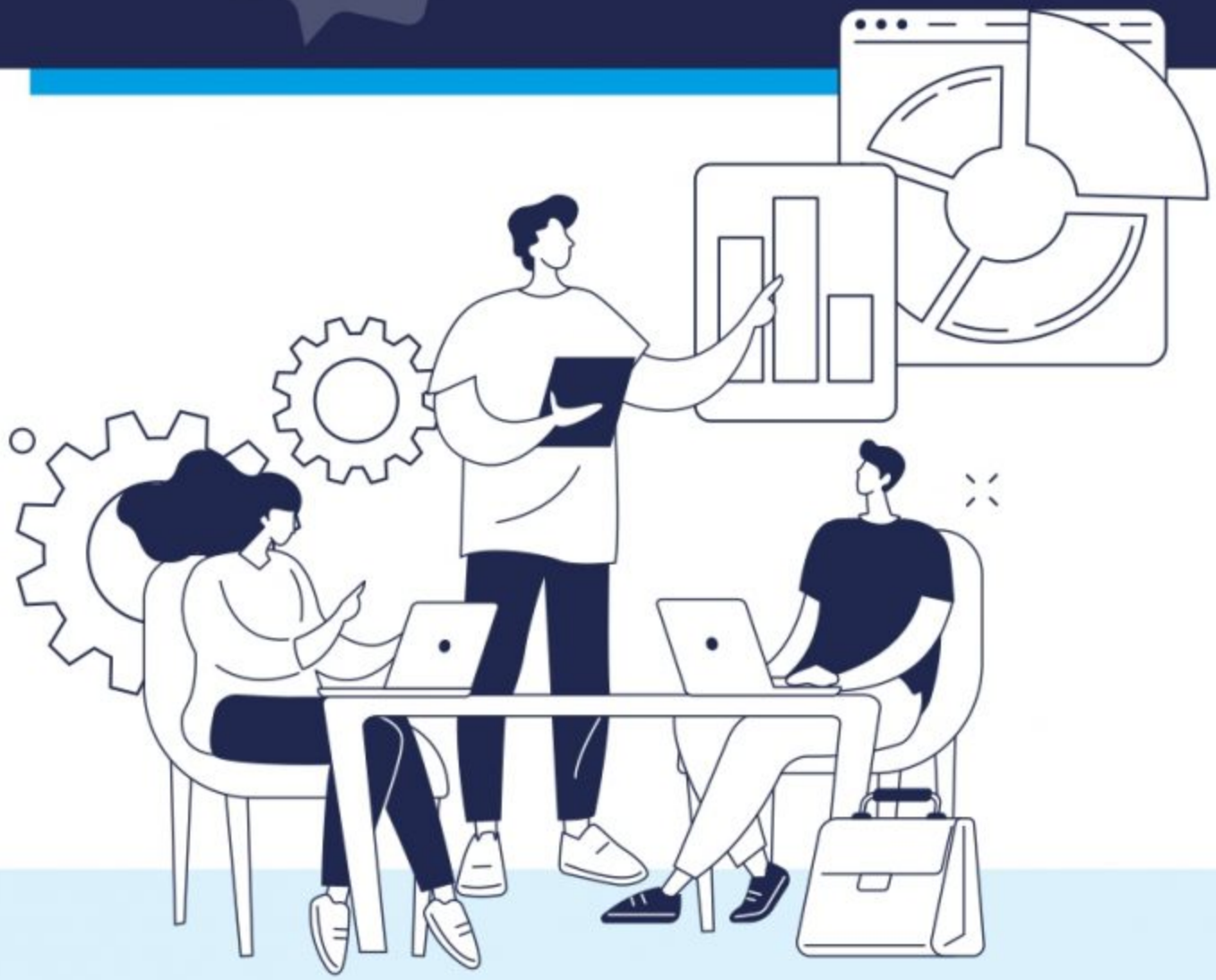
**Зловмисник, який використовує такі відео, може мати на меті наступні наміри:**

1. **Шантаж** (погроза оприлюднити компрометуючий відеозапис особистості).
2. **Шахрайство** (видавання себе за іншу особу з метою отримання доступу до систем або даних).
3. **Автентифікація** (маніпулювання ідентифікаційною перевіркою або автентифікацією, яка використовує біометричні дані як шаблони голосу або розпізнавання обличчя для отримання доступу до систем, даних або інших ресурсів).
4. **Репутаційний ризик** (загроза завдати шкоди репутації особистості чи організації).

З метою уникнення таких вразливостей потрібно прикласти зусилля для розпізнання діпфейків. **Цьому допоможуть наступі методи:**

- Подивіться на неприродні рухи очей.
- Зверніть увагу на невідповідність кольорів і освітлення.
- Порівняйте якість звуку.
- Зауважте дивну форму тіла або рухи.
- Проаналізуйте штучні рухи обличчя.
- Відзначте неприродне розташування рис обличчя.
- Помітно виділяється незручна поза або статура.
- **Діпфейки у реальному часі можна розпізнати, якщо особа поверне свою голову. Це означає, що пряма трансляція діпфейку не може зі 100% вірогідністю обробляти інші частини обличчя.**

# КЕЙСИ ІНФОРМАЦІЙНОГО ВПЛИВУ РФ (ПРАКТИКА ЦЕНТРУ)



# Кампанія з дискредитації українсько-польських відносин “Мобілізація в Польщі”


**Посилання:**

https://t.me/JokerDPR/123

З лютого 2022 року на сайті російського інформаційного агентства «Красная весна» з'явилась інформація про підготовку Міністерством закордонних справ України політичних нот з проханням повернути громадян України призовного віку, де вони посилаються на неназваного представника так званої міліції «днр», та повідомлення російського інформаційного агентства Regnum (наразі повідомлення видалено).

Вже 17.06.2022 у Telegram-каналі «Джокер «днр» о 10:53 було опубліковано повідомлення, направлене на дискредитацію українсько-польських відносин, створення недовіри до української влади, а також поширення відчуття страху за власну безпеку в цільової аудиторії (чоловіки призовного віку, які були змушені покинути Україну через початок повномасштабного вторгнення росії, та члени їх сімей).

**Першоджерело:**

Telegram-канал «Джокер «днр» (понад 92 тис. підписників), частина мережі рф, яка використовується для інформаційного супроводу хакерських атак та розповсюдження отриманих даних за їх результатами.

**Посилання:** https://t.me/JokerDPR/123

Публікація супроводжувалась нібито листом міністра закордонних справ України Дмитра Кулеби, що був адресований міністру закордонних справ Республіки Польща Збігнєву Рау. В самому листі український міністр нібито просить свого колегу депортувати всіх чоловіків призовного віку з території Республіки Польща в Україну для подальшої їх мобілізації.

В той же день Цезарій Нобіс, що позиціонував себе як «польський політик», опублікував серію документів дипломатичних установ України та Республіки Польща й заявив, що було прийняте офіційне рішення про пошук усіх осіб призовного віку, які ухиляються від служби в Збройних силах України. Після чого вже згаданий Telegram-канал послався на публікацію Цезарія Нобіса для підтвердження свого попереднього повідомлення. Надалі «новину» підхопили російські ЗМІ та почали поширювати в інформаційному просторі.

**Основний наратив:**

## «Україна готується мобілізувати чоловіків за кордоном».

**Вид загрози:**

Інформаційна кампанія, направлена на дискредитацію українсько-польських відносин, створення недовіри до української влади, а також поширення відчуття страху за власну безпеку в цільової аудиторії (чоловіки призовного віку, які були змушені покинути Україну через початок повномасштабного вторгнення росії, а також члени їх сімей).

**Обсяг поширення:**

понад 100 тис. переглядів.

Зважаючи на потенційно значний обсяг поширення, Центром було проведено аналіз та встановлено всі елементи й етапи здійснення вищеописаної операції. Після чого Центр звернувся до Міністерства закордонних справ України, в якому отримав підтвердження фейковості зазначеного «листа».

**Тип джерел поширення:**

Російська дезінформаційна мережа, що містить як малі (до 100 тис. підписників), так і великі канали (більше 100 тис. підписників), та Facebook-сторінка польського чиновника Цезарія Нобіса.

**Висновок:**

Описана дезінформаційна кампанія несе деструктивний характер для інформаційної безпеки України та її міжнародних партнерів.

Прийнято рішення про реагування на міжвідомчому та міжурядовому рівні.

**Результат:**

Центром було проінформовано Міністерство закордонних справ України про проведення ІПсО.

Відразу після цього Центр звернувся до Урядового центру безпеки Республіки Польща, якому були направлені аналітичні матеріали з усіма деталями ІПсО.

У результаті Центр та Урядовий центр безпеки через налагоджені комунікаційні канали проінформували громадськість та відповідні державні інституції про проведення ІПсО зі сторони російської федерації, а також нівелювали можливі негативні наслідки.

Однак, попри успішну ліквідацію вищеописаного ворожого ІПсО, ворог не залишив свої намагання дискредитувати Україну в очках польських союзників. Так, зважаючи на відмінність трактування та сприйняття певних моментів у спільній історії України та Республіки Польща, через певний період часу ворог вирішив зіграти саме на цьому, обравши своєю цільовою аудиторією консервативну частину польського населення.

https://twitter.com/RCB_RP/status/1537788674754191360?s=20&t=GSQhB5Qt-1nM-laCWMAHcg

https://t.me/CenterCounteringDisinformation/1851

# Кампанія з дискредитації євроатлантичних прагнень України


**Посилання:**

https://tgstat.ru/channel/CXis8yPFITI5Y2Q6/15587

На приватному Telegram-каналі "С МЕСТА СОБЫТИЙ" (понад 800 тис. підписників) 4-го листопада о 14:12 було опубліковано відеоматеріал під назвою «6 причин, чому Україна не має вступати в НАТО» або «6 reasons why Ukraine should not join NATO».

Метою відео є створення неправдивого образу України та її громадян у європейському інформаційному просторі для дискредитації інтеграції України в НАТО.

Автором відео зазначається European Security & Defence College.

Центр звернувся до European Security & Defence College та отримав підтвердження про їх непричетність до створення й розповсюдження зазначеного відеоматеріалу.

**Першоджерело:**

Приватний Telegram-канал "С МЕСТА СОБЫТИЙ" (понад 800 тис. підписників), частина мережі рф.

**Основний наратив:**

## «Вступ України в НАТО негативно вплине на благоустрій держав-членів».

**Вид загрози:**

Інформаційна кампанія, направлена на дискредитацію України.

**Обсяг поширення:**

- 150 тисяч переглядів;
- 5 каналів розмістили публікацію;
- 290 репостів.

**Тип джерел поширення:**

великий російський канал (понад 800 тис. підписників)

**Висновок:**

Дезінформаційна кампанія не досягла початкової мети — широкого розповсюдження в соціальних мережах, але вона мала потенціал для подальшого поширення, оскільки несла резонансні повідомлення для західних громадян.

**Результат:**

Зазначену інформацію було поширено серед представництв у державах-членах НАТО для нівелювання можливого негативного впливу.

Центр протидії дезінформації також підготував повідомлення для сайту та соціальних мереж Центру

**Посилання:** https://t.me/CenterCounteringDisinformation/3035

Як результат, поширення зазначених повідомлень в міжнародному просторі було припинено на початковому етапі.

# Кампанія з дискредитації допомоги від НАТО


**Посилання:**

https://t.me/breakingmash/39593?singl

У Telegram-каналі Mash о 10:00 03. 11. 2022 було опубліковано матеріал, направлений на дискредитацію ЗСУ, Міністерства охорони здоров'я України та країн-членів НАТО.

**Першоджерело:**

Telegram-канал Mash (більше 1 млн підписників), частина мережі рф.

**Основний наратив:**

## «країни-члени НАТО поставляють Україні консервовану кров, що містить віруси ВІЛ, гепатит В/С та інші інфекції, які можуть призвести до епідемії серед українських військовослужбовців».

Публікація супроводжувалась документами, які нібито були отримані за допомогою хакерської групи Kombatant. Зазначені документи містять підпис міністра охорони здоров'я Віктора Ляшка та згадування особистої поштової скриньки прем'єр-міністра України Дениса Шмигаля.

**Вид загрози:**

Інформаційна кампанія, направлена на дискредитацію ЗСУ та НАТО.

**Обсяг поширення:**

- більше 1-го мільйона переглядів;
- 252 канали розмістили публікацію;
- 20 тисяч репостів.

**Тип джерел поширення:**

Російська дезінформаційна мережа з одним дуже великим каналом (більше 1 мільйона підписників).

**Висновок:**

Описана дезінформаційна кампанія несе деструктивний характер для інформаційної безпеки України та її міжнародних партнерів.

Прийнято рішення про реагування на міжвідомчому рівні, підготовлено та направлено рекомендації до Міністерства охорони здоров'я та Міністерства оборони України.

**Результат:**

Міністерство охорони здоров'я України на своєму офіційному сайті випустило спростування проаналізованої інформації

**Посилання:** https://moz.gov.ua/article/news/sprostovuemo-chergovij-rosijskij-fejk-pro-nejakisnu-krov-dlja-pacientiv.

Центр протидії дезінформації також підготував повідомлення для сайту та соціальних мереж Центру

**Посилання:** https://cpd.gov.ua/warning/dezinformacziya-pro-import-ukrayinoyu-infikovanoyi-krovi/.

У результаті реагування загроза від інформаційної кампанії була нівельована на початкових етапах.

# Кампанія з дискредитації українсько-японських відносин


11.08.2022 року в соціальних мережах Twitter та Instagram було опубліковано матеріал, що направлений на дискредитацію українських біженців, Японської держави, а також українсько-японських відносин загалом.

**Першоджерело:**

Японські бот-акаунти в соціальних мережах Twitter та Instagram.

**Основний наратив:**

## «Світ втомився від війни в Україні».

Публікація супроводжувалась нібито фотографіями рекламного білборда компанії Sushi no midori в місті Токіо, на якому зображується японський кухар-сушист, що затуляє рота українці із закликом: «Давайте змінимо тему — поговорімо про смачні суші».

**Вид загрози:**

Інформаційна кампанія, направлена на дискредитацію українських біженців, Японської держави, а також українсько-японських відносин загалом.

**Обсяг поширення:**

Незважаючи на великий потенціал для розповсюдження, завдяки своєчасній реакції Центру обсяг поширення склав менше 10 тис. переглядів.

**Тип джерел поширення:**

Російська мережа скоординованої неавтентичної поведінки із залученням нішевих російських ЗМІ.

**Висновок:**

Описана дезінформаційна кампанія несе деструктивний характер для інформаційної безпеки України та її міжнародних партнерів.

Прийнято рішення про реагування на міжвідомчому рівні, підготовлено та направлено рекомендації до Міністерства закордонних справ України, а також Посольства України в Японії.

**Результат:**

Посольство України в Японії звернулося до керівництва компанії Sushi no midori для отримання пояснень щодо провокаційного білборда.

Компанія повідомила, що не підтримує дискримінацію жодної з країн чи національностей, а зображення, яке поширюється, не має відношення до їх компанії

**Посилання:** https://www.sushinomidori.co.jp/#modal_1329).

Крім цього, було подано заяву до японської поліції для встановлення всіх обставин справи з подальшим відкриттям кримінального провадження.

Центр протидії дезінформації в свою чергу підготував розвінчання фейку для сайту та соціальних мереж Центру

**Посилання:** https://t.me/CenterCounteringDisinformation/2329).

У результаті реагування загроза від інформаційної кампанії була нівельована на початкових етапах.

# РЕКОМЕНДАЦІЇ ЩОДО ПРОТИДІЇ ШКІДЛИВОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ ТА КОМУНІКАЦІЙ ІЗ ЦІЛЬОВОЮ АУДИТОРІЄЮ

Перш за все, слід розуміти, що не існує єдиної універсальної відповіді на всі інформаційні загрози. Як ви вже могли побачити, інформаційний вплив може приймати найрізноманітніші форми. Крім цього, кожна організація має положення, яке окреслює рамки, в яких вона може виконувати свої функції, і відповідно з цього випливають певні вразливості. Тому інструменти реагування мають бути сформовані відповідно до особливостей організації.

Реагування на інформаційну загрозу має відповідати її рівню. Далі буде представлено узагальнений алгоритм реагування на різних рівнях.

## Реагування на основі фактів

Перші два рівні — оцінювання та інформування. Вони є ключовими для фіксування й повідомлення.

### Рівень 1. Оцінювання.

Для того, щоб зрозуміти, з чим ми маємо справу, необхідно провести оцінку ситуації. Що відбувається? Хто бере в цьому участь? Які ризики випливають із ситуації? Чим більше інформації вдасться зібрати, тим краще буде підібрано необхідне реагування.

#### 1. 1. Аналіз ситуації.

Проаналізуйте та сформуйте повноцінне бачення ситуації. Використовуйте інформацію з попередніх розділів, щоб визначити, з чим ви маєте справу.

### 1.2. Фактчекінг.

Проведіть дослідження фактів — що є правдою, а що дезінформацією.

### 1.3. Всебічність дослідження.

Залучайте надійних експертів для забезпечення всебічного дослідження питання.

## Рівень 2. Інформування.

Після проведення оцінки загрози слід перейти до інформування. Це може бути як комунікація з населенням, так і інформування зацікавлених органів влади для подальшої координації відповіді на загрозу.

### 2.1. Інформування зацікавлених сторін.

Колеги, інші департаменти, інші державні органи — усі зацікавлені сторони мають бути проінформовані якомога швидше, особливо якщо загроза високого рівня та потребує координованої міжвідомчої відповіді.

### 2.2. Офіційна заява.

Скомунікуйте фактичні обставини справи у нейтральному вигляді, якщо йде мова про низький рівень загрози, який потребує реагування на рівні організації. Або ж підготуйте заяву, що ви досліджуєте ситуацію. Це дасть вам час на підготовку ретельнішої відповіді.

### Адвокація

Третій та четвертий рівні мають на меті відстояти та захистити. Ці кроки містять заходи, які підходять у складних ситуаціях, коли було чітко визначено кампанію інформаційного впливу.

## Рівень 3: Відстоювання.

Відстоювання дуже схоже на інформування, проте передбачає активнішу аргументацію. Тут важливо не забувати про цінності організації при формуванні відповіді.

### 3.1. Наратив.

Поєднайте ситуацію з ширшим наративом, наприклад про організацію та її цінності, що допоможе цільовій аудиторії краще зрозуміти суть справи та сформувати власну позицію.

### 3.2. Доступ до інформації.

Спростіть доступ до інформації для вашої цільової аудиторії. Організуйте заходи, зустрічі, пресконференції, щоб обговорити конкретну проблему і надати вам можливість донести позицію організації.

### 3.3. Поширення.

Залучайте ключових фахівців у галузі зв'язків із громадськістю, які можуть допомогти поширити ваш наратив на широку аудиторію.

## Рівень 4.Захист.

Захист передбачає пряму відповідь на дії агресора. Цей крок може здаватися суперечливішим і доступ до нього, як правило, має лише обмежена кількість державних органів.

### 4.1. Скарги.

Якщо шкідливий інформаційний вплив є результатом порушення законів держави або кодексу поведінки соціальної мережі, слід звертатися до правоохоронних органів або адміністрацій платформ з метою видалення публікацій. Даним інструментом не слід зловживати для уникнення негативних публічних дискусій.

### 4.2. Блокування.

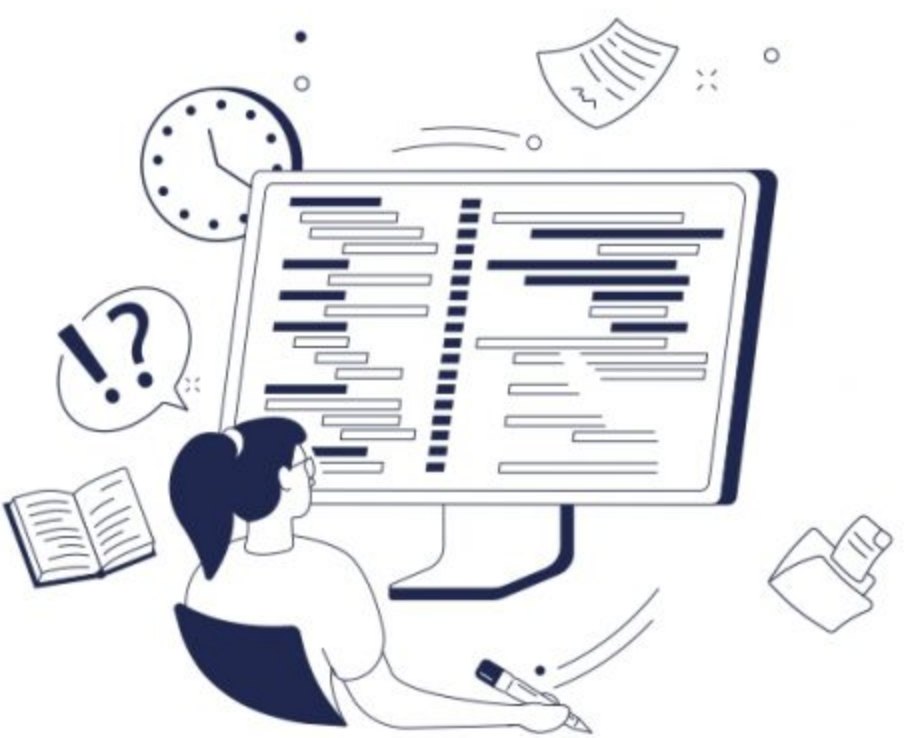
Шкідливий інформаційний вплив певного суб'єкта можете стати причиною його блокування на платформах. Проте таке блокування має бути чітко вмотивоване порушеннями правил платформ. Даний інструмент також несе ряд потенційних ризиків, головним з яких є популярність суб'єкта блокування та його репутація. Якщо він має бездоганну репутацію та є популярним, нічого не заважає йому або створити нову сторінку і швидко відновити аудиторію, або оскаржити рішення, що може стати причиною небажаних публічних обговорень.

### 4.3. Викриття.

Викриття справжніх мотивів, цілей та афіліації суб'єкта шкідливого інформаційного впливу. Розкриття деталей інформаційних кампаній, які він проводить, та їх скоординованості з ворожим актором. Є одним із найдієвіших інструментів реагування на ве-

ликі кампанії з високим рівнем загрози. Однак є певні ризики, для уникнення яких викриття має бути підкріплене всебічним аналізом, який не залишає місяця для спекуляцій.

Вибір найдоречнішого рівня реагування залежить від вашої оцінки ситуації. Якщо ви спостерігаєте низький рівень шкідливого інформаційного впливу — проблему краще за все вирішувати на першому і другому рівнях, тобто інформувати зацікавлені сторони та громадськість неупереджено. Таке реагування базується на фактах. Для складніших випадків — середнього і високого рівнів шкідливого інформаційного впливу, слід використовувати перші два рівні у поєднанні з третім і четвертим, тобто відстоювати позицію та захищати свою організацію від нападів. Однак на цьому етапі слід бути обережним, оскільки з'являється ряд дзеркальних ризиків для організації, тому такі відповіді мають бути ретельно підготовані.



# ГЛОСАРІЙ

**Інформаційний вплив** — цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість особистості, соціальних груп чи населення (корекція поведінки) в інформаційно-технічну інфраструктуру об'єкта впливу та/чи фізичний стан людини.

**Гібридна війна** — війна з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму, кібервійни, торгових війн, патентних війн, реваншистських рухів, пропаганди, порушень прав людини, злочинів проти людяності, військових навчань, переселення, узурпації, вплив на громадську думку, акти цензури та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-агресоркою в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які здобуваються звичайною війною.

**Бот** — спеціальна програма, що виконує автоматично і/або за заданим розкладом які-небудь дії через ті ж інтерфейси, що й звичайний користувач, таким чином імітуючи його.

**Віртуал/сокпапет** — шахрайські облікові записи, якими керує людина анонімно, приховуючи свої наміри. Ці фальшиві особистості використовуються, щоб вступати в інтернет-спільноти та брати участь у дебатах, аби представляти неправдиву чи суперечливу інформацію. Застосовують також два або більше віртуали одночасно, щоб штучно стимулювати обидві сторони дебатів.

**Галоп Гіша** — риторичний прийом, який полягає в тому, щоб «закидати» опонента якомога більшою кількістю аргументів, не звертаючи уваги на їхню точність, обґрунтованість чи релевантність.

**Дезінформація —** неправдива або маніпулятивна інформація, яка навмисно поширюється з метою введення в оману. Дезінформація є наріжним каменем класичної пропаганди та основою сучаснішого явища — фейкові новини.

**Інфоалібі —** це інформаційна маніпуляція, суть якої полягає у превентивному звинуваченні однією стороною іншої в діях, які були/будуть вчинені нею ж. Наприклад, росія звинувачує українську сторону у плануванні обстрілів мирного населення в регіоні, який пізніше буде обстріляно артилерією рф.

**Інформаційна атака —** сукупність навмисних дій зловмисника, спрямованих на порушення однієї з трьох властивостей інформації — доступності, цілісності чи конфіденційності.

**Інформаційна бульбашки/Луна-камери —** органічні підгрупи, в яких люди спілкуються насамперед із тими, хто має аналогічні думки і переконання. Інформаційні бульбашки можна використовувати також для поширення цільової інформації для певних груп або навіть маніпулювати ними для обмеження доступу до джерел інформації, в результаті чого людина опиняється у замкненій системі циркуляції інформації.

**Інформаційна загроза —** потенційна або реальна негативна дія чи подія, спричинена вразливістю, що призводить до небажаного впливу на інформаційний простір.

**Інформаційна кампанія —** це спланований потік інформації з певними цілями та завданнями, що розповсюджується за допомогою різних засобів та каналів масового й індивідуального інформування, і характеризується певною протяжністю у часі та інтенсивністю.

**Інформаційна маніпуляція —** правдива інформація, спотворена з метою впливу на поведінку та судження споживача.

**Інформаційна операція —** заздалегідь спланований та підготовлений акт інформаційного впливу на таргетовану аудиторію, націлений на досягнення певних стратегічних цілей. Інформаційні операції характеризуються короткою протяжністю в часі та відносно невеликим ресурсним забезпеченням.

**Інформаційний простір —** окремий простір людської діяльності, де створюється, змінюється та передається інформація. Це певна історично сформована форма скоординованих та структурованих інформаційних ресурсів, що акумулюють результати комунікаційної діяльності людей. Інформаційним простором може вважатися сукупність баз даних, комунікаційних систем та технологій їх застосування.

**Координована неавтентична поведінка (КНП) —** зловмисна діяльність, що ведеться за допомогою програм, ботів та інших інструментів проведення інформаційних операцій, які видають себе за реальних осіб для подальшого штучного формування необхідної громадської думки та досягнення певних цілей.

**Мережі координованої неавтентичної поведінки (МКНП)** — мережа взаємопов'язаних інструментів КНП, якими володіє певна організована група осіб та використовує їх для досягнення власних цілей шляхом інформаційного впливу на користувачів.

**Меседж (в комунікації) —** окрема одиниця інформації, що передається джерелом для використання одержувачем або групою одержувачів. Меседж може бути доставлено різними способами, включаючи фізичний лист, телефонний дзвінок, публікацією в соцмережах тощо. Крім

цього, меседжем можуть називати заяву, зроблену одним з опонентів проти іншого.

**Місапропріація —** використання фактично правильного контенту, який не пов'язаний з певною проблемою, щоб сформувати хибне уявлення про цю проблему, подію або особу. Наприклад, фейкова новинна стаття може використовувати як докази зображення, пов'язані із геть іншою подією.

**Місінформація —** неправдива інформація, що поширюється без злочинного умислу або наміру ввести в оману. Наприклад, журналістські помилки, чутки та плітки. Зазвичай люди вірять цій інформації та поширюють її.

**Наратив —** спосіб подачі або розуміння ситуації чи серії подій, який відображає та просуває певну точку зору чи набір цінностей.

**Потьомкінські поселення —** фальшиві кампанії, науково-дослідницькі інститути чи аналітичні центри, створені для формування довіри до дезінформації.

**Спіраль мовчання —** теорія масової комунікації, яка застосовується щодо ситуації, коли люди відчувають зростаючу потребу приховувати свої погляди, якщо останні не підтримуються більшістю. Перед тим як висловити свою точку зору щодо певного явища або ситуації, члени аудиторії схильні несвідомо перевіряти, чи поділяються їхні погляди більшістю.

**Фейк (англ. «fake») —** підробка або імітація елементів інформаційного простору. Може існувати у вигляді спотвореної інформації (фейкова новина або публікація), каналу поширення недостовірної інформації (публічна сторінка у соціальних мережах, веб-сайт тощо) або підробної

сторінки певної людини в соціальних мережах, яка створена з метою ввести в оману користувача платформи (боти, тролі тощо).

**Фішинг («Phishing» від англійського слова «fishing» — риболовля) —** шахрайська практика надсилання електронних листів або інших повідомлень, нібито від авторитетних компаній або осіб, з метою спонукання розкрити особисту інформацію, таку як паролі та номери кредитних карток.

**Якщодоізм/Whataboutism (походить від англійського словосполучення «what about» — як щодо) —** дешева риторична тактика, яка полягає у відхиленні критики від себе шляхом помилкових порівнянь з непов'язаними питаннями.

Київ
2023