

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного
підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

до самостійної роботи з дисципліни

«ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор,
завідувач кафедри «Кібербезпека та захист інформації»

Методичні вказівки схвалено на засіданні кафедри «Кібербезпека та захист
інформації»

(Протокол від «06» жовтня 2025 р. № 2)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП

(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

	Вступ	4
1	Теоретичний базис	4
2	Як ефективно опанувати матеріал: практичні поради	6
3	Практичне завдання для магістрів	9
4	Контрольні питання для самоперевірки	10
	Література	10

ВСТУП

Методичні вказівки призначені для самостійного опанування теми 6 дисципліни «Інформаційно-аналітичне забезпечення інформаційної безпеки» - «Інформаційно-психологічне протиборство» магістрами спеціальності F5 Кібербезпека та захист інформації. Вивчення теми «Інформаційно-психологічне протиборство» є актуальним для розуміння важливості людського фактора та вразливостей людини. У сучасному світі межа між кіберпростором та ментальним простором нації фактично стерта. Сучасні гібридні війни довели: можна мати ідеальну систему кіберзахисту, але програти війну, якщо свідомість громадян, військових або управлінців буде деформована за допомогою цілеспрямованого психологічного впливу.

Вивчення теми «Інформаційно-психологічне протиборство» надає інструментарій для:

- здатності розрізняти звичайний інформаційний потік від спланованої інформаційно-психологічної операції на ранніх етапах;
- аналізу того, як певна маніпуляція в ЗМІ може змінити соціальну поведінку або лояльність населення до державних інституцій;
- створення стратегій не лише реагування, а й превентивного захисту (формування стійкості аудиторії).

Опанування цієї теми формує у магістра спеціальності F5 Кібербезпека та захист інформації розуміння того, що інформаційна безпека - це стан захищеності не лише серверів, а й державного суверенітету в інформаційній сфері.

Мета самостійної роботи - формування цілісного уявлення про методи та засоби інформаційно-психологічного протиборства для подальшої розробки систем інтелектуального захисту держави в умовах невизначеності та постійних інформаційних атак.

1. Теоретичний базис

Для ефективного опанування теми «Інформаційно-психологічне протиборство» необхідно детально вивчити ключові поняття й класифікації за такими тематичними блоками:

Блок 1. Сутність інформаційного впливу та його диференціація

Інформаційний вплив визначається як організоване й цілеспрямоване застосування спеціальних інформаційних засобів і технологій з метою внесення деструктивних змін у свідомість особистості, соціальних груп чи населення загалом (для корекції їхньої поведінки), а також в інформаційно-технічну інфраструктуру та фізичний стан людини.

Майбутньому аналітику необхідно чітко розділяти інформаційний вплив на два види:

- ***Інформаційно-технічний вплив*** (ІТВ), який спрямований на інформаційно-технічну інфраструктуру (сервери, мережі, програмне забезпечення) для порушення її функціонування (зупинка роботи системи, НСД, спотворення даних, програмування помилок, зниження швидкості обробки). Безпека інфраструктури тут поділяється на безпеку

машинно-технічних засобів, безпеку ПЗ та режим захисту від несанкціонованого витоку даних;

- **Інформаційно-психологічний вплив** (ІПсВ), який спрямований безпосередньо на свідомість окремої людини й населення загалом для трансформації їхнього світогляду, поглядів, ціннісних орієнтацій та модифікації поведінки відповідно до цілей суб'єкта впливу.

Блок 2. Механізми базових методів впливу: переконання – навіювання.

Здобувачі мають розуміти алгоритми функціонування двох полярних методів:

- **Переконання:**

- Логіка викладу обов'язково має відповідати інтелектуальному рівню об'єкта.
- Базується на фактах, які вже відомі та верифіковані об'єктом.
- Повинно містити логічно несуперечливі конструкти та загальні пропозиції.
- Потребує відповідного емоційного забарвлення фактів для кращого закріплення.

- **Навіювання:**

- Це пряме вторгнення у психіку через зниження рівня усвідомленості. Сприйняття інформації відбувається без розгорнутого логічного аналізу, діючи як безпосередня інструкція до дії.
- Має чітку селективність — розраховане на конкретні групи населення з урахуванням їхніх соціально-психологічних або національних особливостей.
- Повністю орієнтоване на емоційну сферу, де функціонують лише процеси сприйняття й запам'ятовування, а мислення залишається пасивним. Осмислення такої інформації відбувається значно пізніше.

Необхідно чітко визначити фактори, що визначають ефективність ІПсВ:

- *Зміст матеріалу:* чим простіша інформація та конкретніший заклик до дії, тим вищий рівень автоматизму реакції аудиторії;
- *Психічний стан об'єкта:* перебування у стані страху, апатії чи пригніченості значно знижує критичність мислення;
- *Часовий інтервал:* чим більше часу проходить між моментом отримання повідомлення та дією, тим нижчим є автоматизм реакції, оскільки людина встигає «включити» критичне мислення.

Блок 3. Структура джерел загроз інформаційно-психологічній безпеці.

Необхідно засвоїти трирівневу класифікацію джерел загроз у комунікації:

- *Загрози процесу комунікації:* можливість маніпулятора штучно змінювати хід, процедуру, часові межі та інформаційне наповнення діалогу чи ефіру;
- *Загрози зовнішніх чинників:* використання статусних переваг маніпулятора (посада, вік, фінансове становище, освіта), специфіки

фізичного середовища (час, місце, обстановка) чи існуючих соціальних зв'язків у середовищі адресата;

- *Загрози внутрішніх чинників*: експлуатація індивідуально-особистісних рис самого адресата, його психологічного стану, біосоціальної природи психіки та вразливостей сприйняття.

Блок 4. Політичне маніпулювання та методи викривлення інформації.

На відміну від міжособистісного впливу, політичне маніпулювання є знеособленим масовим процесом, де воля меншості завуальовано нав'язується більшості з метою уніфікації способів мислення («роботизація» та деперсоніфікація мас).

Магістр повинен детально розібрати три базові методи маніпулювання даними:

- *Перекручування інформації*: спектр дій від відвертої дезінформації (брехні) до підтасовування реальних фактів і штучного зміщення понять у семантичному полі;
- *Приховування інформації*: повне замовчування критично важливих тем, або метод дозованого, часткового чи диференційованого висвітлення матеріалу;
- *Спосіб подання інформації*: використання прийому «інформаційного потопу» (подача гігантського обсягу несистематизованих, «сирих» даних, що забиває ефір і унеможливорює пошук суті) або навпаки - видача мікроскопічних порцій, якими неможливо скористатися. Окремим інструментом є особливе компоновання тем, яке підштовхує аудиторію до потрібного маніпулятору висновку.

2. Як ефективно опанувати матеріал: практичні поради

Для глибокого розуміння природи інформаційно-психологічного протистояння, під час самостійної роботи рекомендується сконцентрувати фокус на аналізі реальних механізмів впливу:

- *Навчіться бачити «друге дно» технічних атак*, не сприймайте кібератаки лише як збої в коді. У гібридній війні злам сервера часто лише є початком для психологічної операції. При вивченні будь-якого технічного впливу необхідно контролювати те, який емоційний стан у суспільства може викликати цей злам. Інформаційно-психологічна операція обов'язково включає як психологічну, так і технічну складові;
- Інформаційно-психологічний вплив – це *розум проти емоцій*. Фахівцю з кібербезпеки та захисту інформації важливо розуміти: якщо новина змушує відчувати лють або паніку ще до того, як ви вчиталися в цифри, це класичний приклад навіювання, переконання ж використовує логіку (цифри, аргументи). Опрацьовуючи розділ теми 6, який стосується питань переконання та навіювання, для кращого його розуміння спробуйте знайти їхні сліди у вчорашніх стрічках новин. Опанувавши попередньо теми 1-5 курсу і маючи розуміння, що для інформаційно-аналітичного забезпечення інформаційної безпеки треба не тільки знайти, а й проаналізувати інформацію, скласти доказову базу, рекомендується:

- Коли ви знайшли приклад навіювання або викривленого переконання, розкладіть його на три складові: «стимул – реакція - мета», тобто яке слово, образ чи цифра викликали емоцію (наприклад: використання слова «геноцид» замість «економічна криза» - це перехід від логіки до чистого емоційного навіювання); на який «базовий страх» чи стереотип аудиторії це розраховано (наприклад, страх за майбутнє дітей, мовне питання, недовіра до влади); яку дію має вчинити людина після прочитання (наприклад, вийти на мітинг, забрати гроші з банку, не йти на вибори).
- Оскільки магістрам спеціальності F5 Кібербезпека та захист інформації в межах вивчення курсу «Інформаційно-аналітичне забезпечення інформаційної безпеки» важливо зафіксувати це як інформаційний інцидент, спробуйте оформити свої знахідки у вигляді аналітичної таблиці:

Компонент аналізу	Опис (Ваше спостереження)
Джерело	Конкретне ЗМІ, Telegram-канал або лідер думок.
Метод	Навіювання (емоції) чи маніпулятивне переконання (викривлені факти).
Техніка	Наприклад: «Напівправа», «Створення загрози», «Апеляція до авторитету».
Очікуваний ефект	Поширення паніки, дезорієнтація, дискредитація держорганів.

- Подивіться на цю новину очима фахівця з кібербезпеки та захисту інформації: чи достатньо в цій ситуації простого спростування (фактчекінгу); чи потрібно проводити власну контр-операцію (наприклад, зміщувати акцент з емоцій на цифри); чи цей вплив настільки токсичний, що потребує адміністративного реагування (блокування джерела).
Рекомендація: спробуйте взяти одну й ту саму подію (наприклад, прийняття нового закону) і порівняти, як її подають два різні за поглядами ресурси. Це дасть змогу побачити, як з одних і тих самих фактів за допомогою «навіювання» та «переконання» можуть бути сконструйовані дві різні реальності;
- Магістр з кібербезпеки та захисту інформації повинен розуміти, що захист свідомості не може бути забезпечений універсально і миттєво. Захист індивідуальної свідомості (наприклад, керівника відомства) потребує методів інформаційної, психологічної гігієни. Захист масової свідомості вимагає стратегічних комунікацій та роботи зі ЗМІ. Під час опанування теми 6 зверніть увагу, що неможливо захистити націю тільки тими самими методами, якими ми захищаємо окрему людину, оскільки існує різниця між психологією особистості та психологією мас. З погляду інформаційно-аналітичного забезпечення інформаційної безпеки ця різниця стосується

трьох площин: механізми сприйняття, швидкість реакції та інструменти захисту. Саме:

- окрему особистість можна навчити методам фактчекінгу, цифровій гігієні та критичному аналізу. Вона здатна зупинитися, перевірити джерело і зробити раціональний висновок. Захист окремої людини - це інтелектуальна вправа. Велика група людей під впливом інформаційно-психологічної операції часто втрачає здатність до індивідуального аналізу, маса починає реагувати не на логічні аргументи, а на символи та емоційні наративи;
- щоб захистити окремо людину, ставляться фільтри на її пошту, видаляються шкідливі додатки тощо. Все це є персональною гігієною. По нації інформаційно-психологічна зброя б'є через культуру, ЗМІ, релігію, соціальні стандарти та історичну пам'ять. Захистити націю не можна через блокування одного сайту, треба вибудувати стратегічні комунікації, які формують національну ідентичність. Це - ідеологічна архітектура;
- Різниця в методах реагування полягає в наступному: для спростування фейку для окремої людини достатньо надіслати цю інформацію на офіційний реєстр, але для маси людей просте спростування часто не спрацьовує, а іноді навіть шкодить (ефект зворотного вогню), бо лише привертає увагу до брехні. Для захисту нації держава має не виправдовуватися, а створювати свій потужний порядок денний, який витіснить ворожий вплив.

Висновок: індивідуальна безпека - це про правду, національна інформаційно-психологічна безпека - це про довіру. Якщо ворог зруйнує довіру до інституцій, жодні правдиві цифри Держстату не врятують країну від хаосу. Саме тому аналітик інформаційної безпеки має розробляти різні сценарії: як захистити «голову» (керівника) і як захистити «серце» (суспільство).

- ЗМІ сьогодні часто виступають не просто джерелом інформації, а інструментом її інтерпретації. Вивчаючи тренди розвитку сучасних медіа, зверніть увагу на техніки «промивання мізків». Виберіть 2-3 техніки (наприклад, «наклеювання ярликів», «використання авторитетів», «напівправа» тощо) і спробуйте знайти їх у виступах сучасних політиків. Це є практика для аналітика інформаційної безпеки. При цьому треба вміти знаходити маркери маніпулятивного впливу:

– *Організаційні ознаки:*

- *Синхронність появи:* ідентична інформація з маніпулятивними тезами одночасно з'являється у багатьох непов'язаних джерелах, що свідчить про наявність єдиного координаційного центру. Іноді фіксуються аномалії, коли матеріал із посиланням на першоджерело виходить раніше, ніж саме першоджерело його опублікувало;
- *Штучний «Agenda» (порядок денний):* нав'язування суспільству чіткого переліку тем та порядку їх обговорення (наприклад, через «темники» чи штучне акцентування виключно на конфліктних внутрішньодержавних питаннях);

- *Маніпуляція часом виходу*: публікація компрометуючих чи резонансних матеріалів розраховується так, щоб об'єкт не мав фізичної можливості оперативно відповісти, або коли ця відповідь уже не буде почута суспільством (наприклад, під час перебування лідерів за кордоном чи у вихідні дні);
 - *Використання спеціалізованих майданчиків*: первинне оприлюднення чутливої інформації через анонімні веб-сайти, Telegram-канали або платформи для «зливу» компромату;
 - *Специфічні спікери*: залучення до озвучування інформації «шоуменів від політики» або скандально відомих осіб, чиє завдання - викликати бурхливу емоційну реакцію та хаотизувати дискусію.
- *Змістові ознаки*:
- *Контекст тотального страху й невизначеності*: створення загального інформаційного фону, що транслює розгубленість, безвихідь та багатоваріантність загроз, руйнуючи природне прагнення людини до стабільності й безпеки;
 - *Емоційні штампи та кодові слова*: штучне насичення тексту високою концентрацією слів-маркерів з негативним забарвленням («зрада», «катастрофа», «терор», «корупція», «нацизм») для блокування логіки, а також аномально висока кількість прикметників порівняно з іменниками та дієсловами (ознака оціночності замість мови фактів);
 - *Експлуатація «ідеальних понять»*: апелювання до абсолютних категорій (свобода, демократія, справедливість, бог) без зв'язку з реальним контекстом для маскування справжньої (часто агресивної чи прагматичної) мети повідомлення;
 - *Анонімність та псевдоавторитети*: використання розмитих конструкцій типу «за повідомленням нашого поінформованого джерела», «у кулуарах ходять чутки» або неконкретних посилань на авторитети («як доведено світовими вченими», «експерти ФБР вважають») без зазначення конкретних прізвищ чи звітів;
 - *Голослівні твердження*: застосування безальтернативних директивних штампів, що подаються як аксіома без жодної аргументації чи доказової бази («у нас завжди так», «Україна відстала на десятиріччя»).
- інформаційно-психологічний захист - це не «фаєрвол». Це постійний процес формування критичного мислення та стійкості. Аналітик має не просто «блокувати» негатив, а розуміти, як мінімізувати його руйнівний ефект на свідомість об'єкта.

3. Практичне завдання для магістрів

На основі самостійно вивченого матеріалу для його закріплення (та отримання додаткових балів) підготувати аналітичну довідку щодо конкретного випадку інформаційної атаки (кейс на вибір):

1. Описати об'єкт впливу (масова чи групова свідомість).
2. Ідентифікувати використані методи (навіювання, маніпулювання, дезінформація тощо).

3. Запропонувати заходи інформаційно-психологічного захисту для нейтралізації наслідків цієї атаки.

4. Контрольні питання для самоперевірки

1. Чим відрізняється інформаційна зброя від звичайних засобів ураження?
2. Які ознаки вказують на те, що проти населення проводиться саме ІПсО?
3. У чому полягає складність захисту групової свідомості порівняно з індивідуальною?
4. Яка роль соціальних мереж у трансформації сучасного інформаційного протиборства?

Література

Базова:

1. Інформаційна безпека у контексті сучасних технологій інформаційно-психологічного протиборства. Навчальний посібник / В.Петрик, О.Назаренко. – Центр навчальної літератури, 2025. 258 с.
2. Теорія та практика сучасного інформаційно-психологічного протиборства. Навчальний посібник. / В.М.Петрик, С.О.Гнатюк. – Полтава, 2022. 328 с.
3. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. — К.: ПАТ «ВІПОЛ», 2018. – 386 с.
4. Історія інформаційно-психологічного протиборства: підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.
5. Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія/ В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.

Допоміжна:

6. Марків О. Інформаційно-психологічні операції: поняття, види, способи використання в умовах гібридної війни / О. Марків // Гібридна війна і журналістика. Проблеми інформаційної безпеки / за заг. ред. В.О. Жадька. – Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. - С. 229-245.
7. Петрик В. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу / В. Петрик // Сучасні

інформаційні технології у сфері безпеки та оборони. – 2009. – №3(6). – С. 71-75.

8. Гусаров В. Сили інформаційних операцій Росії: якою має бути відповідь України?
9. Панченко В.М. Інформаційні операції в системі стратегічних комунікацій / В. М. Панченко // Стратегічні комунікації. – 2016. – №4. – С. 72-79.
- 10.Отрешко В. Інформаційна безпека в контексті мовних пріоритетів українського державотворення/ В.Отрешко // Гілея: науковий вісник: збірник наукових праць.– К. : Видавництво “Гілея”, 2014