



**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ТА ІННОВАЦІЙНОЇ ОСВІТИ
КАФЕДРА АДМІНІСТРАТИВНО-ПРАВОВИХ ДИСЦИПЛІН ТА
ПУБЛІЧНОГО УПРАВЛІННЯ**

**МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДЛЯ ПРОВЕДЕННЯ СЕМІНАРСЬКИХ ТА ПРАКТИЧНИХ
ЗАНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ІНФОРМАЦІЙНА ГІГІЄНА ТА ПРОТИДІЯ
ДЕЗІНФОРМАЦІЇ»**

*для здобувачів першого (бакалаврського) рівня вищої освіти
галузі знань D Бізнес, адміністрування та право*

УДК 004.056:32.019.5
Т 66

*Схвалено Науково-методичною радою
Дніпровського державного
університету внутрішніх справ
(протокол № 9 від 21.05.2025 р.)*

РЕЦЕНЗЕНТИ:

Таїсія КРУШЕЛЬНИЦЬКА, професор кафедри менеджменту, публічного управління та адміністрування Дніпровського державного аграрно-економічного університету, доктор наук з державного управління, професор;

Сергій КОРІЄВСЬКИЙ, доцент кафедри публічного управління та права Українського державного університету науки і технологій, доктор наук з державного управління.

УКЛАДАЧ:

Мирослав ТРЕЩОВ, професор кафедри адміністративно-правових дисциплін та публічного управління Дніпровського державного університету внутрішніх справ, доктор наук з державного управління, доцент.

Т 66 Трещов М. М. Методичні рекомендації для проведення семінарських та практичних занять з навчальної дисципліни «Інформаційна гігієна та протидія дезінформації» для здоб. перш. (бакалаврського) рівня вищ. освіти галузі знань D Бізнес, адміністрування та право. Дніпро : ДДУВС, 2025. 28 с.

Методичні рекомендації для проведення семінарських та практичних занять з тем, передбачених навчальним планом з навчальної дисципліни «Інформаційна гігієна та протидія дезінформації».

Для здобувачів першого (бакалаврського) рівня вищої освіти.

ЗМІСТ

ВСТУП	4
ТЕМА 1. Загрози людині та суспільству в інформаційній сфері.....	6
ТЕМА 2. Основи інформаційної гігієни.....	7
ТЕМА 3. Поняття, сутність та елементи інформаційно-психологічної операції.....	9
ТЕМА 4. Методологія виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру.....	11
ТЕМА 5. Інструменти протидії дезінформації та деструктивним комунікаційним кампаніям в публічному просторі.....	14
ТЕМА 6. Діяльність та взаємодія органів виконавчої влади з питань національної безпеки в інформаційній сфері.....	16
ТЕМА 7. Аналіз подій і явищ в сучасному інформаційному просторі України.....	19
ТЕМА 8. Державна політика кібербезпеки.....	21
ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ	24

ВСТУП

Метою вивчення дисципліни «Інформаційна гігієна та протидія дезінформації» є формування системи знань та навичок щодо особистої інформаційної гігієни, протидії поточним і прогнозованим загрозам в інформаційній сфері, забезпечення інформаційної безпеки, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям в публічному просторі, запобігання спробам маніпулювання громадською думкою.

Завдання:

знати: основи інформаційної гігієни, концептуальні підходи у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям, особливості діяльності та взаємодії органів виконавчої влади щодо забезпечення інформаційної безпеки, правове та наукове забезпечення виявлення та протидії дезінформації, систему стратегічних комунікацій, положення Стратегії інформаційної безпеки України;

уміти: застосовувати інструменти покращення особистої інформаційної гігієни, досвід інших держав і міжнародних організацій з протидії дезінформації для підготовки пропозицій щодо його використання в Україні, методи виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру; визначати дезінформацію та інші маніпулятивні інформаційні матеріали; здійснювати узагальнення, аналіз та оцінку інформаційних загроз з метою оперативного реагування на них.

Вивчення дисципліни «Інформаційна гігієна та протидія дезінформації» має численні переваги. Перш за все дана навчальна дисципліна сприяє розвитку критичного мислення, адже здобувачі навчаються аналізувати інформацію та вміння відрізнити правдиві факти від маніпуляцій або фальшивих новин. Це надзвичайно важливо в умовах сучасного інформаційного середовища, де ми постійно стикаємося з величезними обсягами даних.

Знання основ інформаційної гігієни також допомагає захистити себе та своє оточення від наслідків дезінформації. Вміння ідентифікувати маніпуляції, які можуть впливати на суспільну думку або створювати паніку, є важливою складовою сучасної інформаційної безпеки.

Ця навчальна дисципліна підвищує медіаграмотність здобувачів, навчаючи їх правильно взаємодіяти з медіа, перевіряти достовірність джерел та оцінювати надійність інформації, що поширюється через різні канали. Вона також допомагає покращити комунікаційні навички, адже знання принципів інформаційної гігієни дозволяє більш ефективно та відповідально комунікувати в публічному просторі, знижуючи ризики поширення неперевіраних або хибних даних.

У результаті вивчення навчальної дисципліни здобувачі набувають усвідомлення важливості відповідальності за інформацію, адже кожен може бути як джерелом, так і споживачем інформації. Це знання допомагає їм ставати більш обізнаними та відповідальними у виборі та розповсюдженні інформаційних матеріалів.

Окрім того, володіння знаннями в галузі інформаційної гігієни розширює можливості для професійного розвитку, адже такі навички є надзвичайно важливими в медіа, маркетингових, PR та інших сферах, де критично важлива правильна робота з інформацією.

Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою:

Інтегральна компетентність – здатність розв’язувати складні спеціалізовані завдання та практичні проблеми у сфері публічного управління та адміністрування або у процесі навчання, що передбачає застосування теорій та наукових методів відповідної галузі і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК4 – Здатність бути критичним і самокритичним.

ЗК5 – Здатність до адаптації та дії в новій ситуації.

ЗК8 – Вміння виявляти, порушувати та вирішувати проблеми.

ЗК9 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні компетентності:

СК2 – Здатність забезпечувати належний рівень вироблення та використання управлінських продуктів, послуг чи процесів.

СК4 – Здатність використовувати в процесі підготовки і впровадження управлінських рішень сучасні ІКТ.

СК6 – Здатність здійснювати інформаційно-аналітичне забезпечення управлінських процесів із використанням сучасних інформаційних ресурсів та технологій.

СК13 – Здатність до стратегічного та аналітичного мислення, управління проектами та ризиками.

СК14 – Здатність до політичної і соціальної ерудиції, креативності.

До дисципліни «Інформаційна гігієна та протидія дезінформації» віднесено такі ***програми результати навчання (ПРН):***

ПРН8 – Розуміти та використовувати технології вироблення, прийняття та реалізації управлінських рішень.

ПРН11 – Уміти здійснювати пошук та узагальнення інформації, робити висновки і формулювати рекомендації в межах своєї компетенції.

ПРН12 – Уміти налагодити комунікацію між громадянами та органами державної влади і місцевого самоврядування.

Таким чином, здобувачі отримають комплексні знання та навички, які дозволяють ефективно аналізувати, оцінювати та фільтрувати інформацію в умовах інформаційного середовища, що постійно змінюється. Вони зможуть критично підходити до споживання інформації, відрізняти достовірні джерела від маніпуляцій та дезінформації, а також забезпечувати свою інформаційну безпеку та безпеку оточення. Окрім того, здобувачі набудуть практичних навичок для ефективної комунікації в публічному просторі, що дозволить їм бути відповідальними та обізнаними учасниками інформаційних процесів. Ці знання та вміння відкривають нові можливості для професійного зростання в різних сферах, де важлива грамотність у роботі з інформацією.

ТЕМА 1. ЗАГРОЗИ ЛЮДИНИ ТА СУСПІЛЬСТВУ В ІНФОРМАЦІЙНІЙ СФЕРІ

Зміст теми:

Базові поняття щодо інформації. Принципи інформаційних відносин. Суб'єкти та об'єкт інформаційних відносин. Інформаційна діяльність. Інформаційний суверенітет людини. Інформаційна сфера та її безпека. Інформаційна безпека суспільства. Інформаційно-психологічна безпека особистості.

Семінарське заняття – 2 год.

План:

1. Інформаційний суверенітет людини.
2. Інформаційна сфера та її безпека.
3. Інформаційна безпека суспільства.
4. Інформаційно-психологічна безпека особистості.

Рекомендована література:

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL : <https://zakon.rada.gov.ua/laws/show/2297-17>.
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL : <https://zakon.rada.gov.ua/laws/show/2657-12>.
3. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. та ін. Інформаційна безпека: підручник. К. : Ліра-К, 2021. 412 с.

ТЕМА 2. ОСНОВИ ІНФОРМАЦІЙНОЇ ГІГІЄНИ

Зміст теми:

Поняття «інформаційна гігієна». Принципи критичного мислення. Принципи інформаційної гігієни. Основні правила інформаційної гігієни. Наслідки неправильної інформаційної гігієни. Шляхи покращення інформаційної гігієни.

Семінарське заняття – 2 год.

План:

1. Основні правила інформаційної гігієни.
2. Наслідки неправильної інформаційної гігієни.
3. Шляхи покращення інформаційної гігієни.

Практичне заняття – 2 год.

План:

Робота із ситуаційними вправами щодо покращення інформаційної гігієни.

Практичні завдання:

Завдання. Фішинг: розпізнавання підозрілих електронних листів.

Ознайомтесь із наведеним нижче прикладом фішингового листа.

«Тема: Ваш обліковий запис заблоковано! Дій зараз, щоб відновити доступ.

Шановний користувачу!

Ми помітили підозрілі спроби входу у ваш обліковий запис на нашій платформі. Для вашої безпеки ваш обліковий запис було тимчасово заблоковано. Щоб відновити доступ, вам потрібно терміново підтвердити свою особистість та змінити пароль.

Кроки для відновлення доступу:

Перейдіть за наступним посиланням: Відновити доступ

Введіть свої дані для входу.

Змініть свій пароль на новий.

Зверніть увагу, що якщо ви не виконаєте ці кроки протягом 24 годин, ваш обліковий запис буде остаточно заблоковано.

Якщо ви не здійснювали спробу входу або вважаєте цей лист помилковим, будь ласка, надайте нам відповідь.

З найкращими побажаннями

Команда підтримки АО Барабука»

Виявіть ознаки фішингу (помилки в адресі, підозрілі посилання, нетиповий стиль листа). Оцініть ризики і сформулюйте рекомендації для уникнення подібних ситуацій.

Рекомендації щодо організації процесу виконання цього завдання:

1. Аналіз фішингових листів.

Почніть з уважного вивчення наданого фішингового листа. Пошукайте ознаки, які можуть свідчити про фішинг: підозрілі посилання або адреси відправника; невідповідність між доменом та компанією, що вказана в листі; запити на особисті дані, паролі, фінансову інформацію; спамові фрази, такі як «дійте негайно», «ваш обліковий запис заблоковано»; перевірте кожен елемент листа: текст, формат, стиль написання, відсутність персоналізації.

2. Дослідження безпеки сайтів.

Якщо фішинговий лист містить посилання, використовуйте онлайн-інструменти для перевірки URL, щоб перевірити безпеку сайту. Оцініть, чи виглядає сайт схожим на офіційний, зверніть увагу на дрібні помилки, такі як неправильне написання домену.

3. Створення рекомендацій щодо безпеки.

Після виявлення ознак фішингових атак розробіть рекомендації, як уникнути подібних загроз:

- завжди перевіряйте URL-адреси та авторитетність джерела перед натисканням на посилання;
- використовуйте складні паролі і змінюйте їх регулярно;
- активуйте двофакторну автентифікацію на всіх важливих облікових записах;
- уникайте введення особистої інформації на підозрілих і незнайомих сайтах.

4. Ознайомлення з реальними прикладами.

Вивчіть реальні приклади фішингових атак на сайти великих компаній або урядових порталів.

Зробіть висновки щодо того, чому ці атаки стали можливими і що можна зробити, щоб уникнути подібних ситуацій.

Оцініть, які наслідки мали ці атаки для користувачів і організацій.

5. Підготовка до обговорення.

Подумайте про питання, які можуть виникнути під час обговорення (наприклад, що робити, якщо ви стали жертвою фішингової атаки або як навчити інших уникати подібних помилок).

Рекомендована література:

1. Мунько А. Ю., Саліпа О. І. Комунікаційна стратегія: від політики до публічного управління. Актуальні питання сучасної науки та освіти: матер. Міжнар. наук.-практ. конф. (м. Львів, 2-3 березня 2020 р.). Львів : Львівський науковий форум, 2020. С. 9-10.

2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. та ін. Інформаційна безпека: підручник. К. : Ліра-К, 2021. 412 с.

3. Педорич А. Інформаційна гігієна як основа здорового способу життя. *Вісник національного університету «Чернігівський колегіум» імені Т. Г. Шевченка*. 2024. № 25(181). С. 226-231. URL : <https://visnyk.chnpu.edu.ua/index.php/visnyk/article/view/717/755>.

4. Трещов М. М., Наумик А. С. Цифровізація воюючої держави: необхідність та переваги. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. № 9.

ТЕМА 3. ПОНЯТТЯ, СУТНІСТЬ ТА ЕЛЕМЕНТИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ОПЕРАЦІЇ

Зміст теми:

Типи психологічних операцій: стратегічні, оперативні та тактичні. Поняття «інформаційно-психологічної операції». Елементи інформаційно-психологічної операції. Засоби інформаційно-психологічної операції. Дезінформація та її просування. Пропаганда та контрпропаганда. Інформаційно-психологічні операції у війнах та збройних конфліктах другої половини XX – початку XXI ст.

Семінарське заняття – 2 год.

План:

1. Засоби інформаційно-психологічної операції.
2. Дезінформація та її просування.
3. Пропаганда та контрпропаганда.

Практичне заняття – 2 години

План:

1. Загальний огляд системи інформаційної пропаганди рф.
2. Інформаційно-психологічні операції рф в Україні.
3. Інформаційна кампанія з протидії використанню теми «російського спорту» в пропаганді рф.

Практичні завдання:

Завдання. Обрати один із прикладів російської інформаційно-психологічної операції в Україні та здійснити опис її особливостей за довільною формою (1-2 сторінки А4).

Рекомендації щодо організації процесу виконання цього завдання:

1. Вибір прикладу інформаційно-психологічної операції (ІПСО).

Перш за все вам потрібно вибрати конкретний приклад російської інформаційно-психологічної операції в Україні. Це може бути одна з наступних операцій:

- пропагандистські кампанії через соціальні мережі;
- поширення фейкових новин або маніпуляція фактами щодо війни в Україні;
- створення інформаційних конфліктів серед українців через маніпуляції або підбурювання до протестів;
- використання підроблених або змінених відео, аудіо або інших мультимедійних матеріалів для дискредитації української влади або військових;
- операції з інформаційним впливом через російські медіа-канали на теренах України.

2. Опис особливостей обраної операції.

Коли виберете приклад, опишіть характеристики та особливості ІПСО:

- цілі та завдання операції (Які основні цілі переслідувалися? Наприклад, створення паніки, поширення неправдивої інформації, маніпулювання громадською думкою, вплив на політичні настрої);
- механізми та інструменти впливу (Як саме проводилась операція? Які канали використано, як-от: телебачення, соцмережі, месенджери, пропагандистські видання тощо);
- цільова аудиторія (Кого намагалися переконати або маніпулювати? Наприклад, це могла бути українська аудиторія, міжнародна спільнота, або навіть внутрішні еліти та політики);
- техніки і методи (Опишіть, які психологічні методи та технології були використані: маніпулювання емоціями, створення фейкових новин, використання страшилок або вигадок, створення «віртуальних ворогів» тощо).

3. Аналіз ефективності.

Після опису операції проаналізуйте її ефективність:

- Як вона вплинула на українське суспільство?
- Чи були наслідки операції в політичному або соціальному контексті?
- Чи вдалося досягти поставлених цілей? Можна оцінити успіх операції через зміну настроїв у суспільстві, зростання пропагандистських настроїв або поширення фейків.

4. Рекомендації щодо захисту.

Сформулюйте, які рекомендації можна надати для протидії подібним операціям? Це можуть бути конкретні поради для державних структур, медіа, організацій громадянського суспільства чи навіть кожного громадянина.

5. Висновки.

Висновок має містити загальну оцінку ефективності операції та пропозиції щодо майбутніх кроків для протидії таким діям з боку ворога.

6. Дотримуйтесь вимог оформлення: Times New Roman 14 пт. Міжрядковий інтервал 1,5. Поля: зверху, знизу - 2 см, ліве - 3 см, праве - 1 см.

Рекомендована література:

1. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни: аналіт. звіт. К. : ГО «Український інститут медіа та комунікації», 2023. 66 с.

2. Кучеренко А. Інформаційно-психологічні операції росії в державах «Глобального Півдня» (дослідж. в рамках проекту «Посилення аналітичних спроможностей прийняття рішень у сфері зовнішньої політики за допомогою громадянського суспільства». К. : Аналітичний центр ADASTRA, 2023. 19 с. URL : https://analytics.intsecurity.org/wp-content/uploads/2023/12/Ukr_ADASTRA_11_Global-South.pdf.

3. Солонько О. Інфодемія. Зброя дезінформації у вірусну епоху. К. : Markobook, 2023. 392 с.

4. Центр протидії дезінформації. URL : <https://cpd.gov.ua>.

ТЕМА 4. МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗЛИВИХ ІНФОРМАЦІЙНИХ МАТЕРІАЛІВ МАНІПУЛЯТИВНОГО ТА ДЕЗІНФОРМАЦІЙНОГО ХАРАКТЕРУ

Зміст теми:

Правила та труднощі визначення дезінформації. Правове регулювання медіаграмотності: основні компетентності. Перевірка джерела інформації. Перевірка на послідовність і підтвердження інформації. Перевірка фактів і оцінка доказів дезінформації. Поширення дезінформації в соціальних мережах. Протидія дезінформації на платформі, де вона поширюється. Теорії змови та боротьба з ними. Посилення стійкості населення України до дезінформаційних впливів та розвиток відповідального медіаспоживання.

Семінарське заняття – 2 год.

План:

1. Перевірка фактів і оцінка доказів дезінформації.
2. Поширення дезінформації в соціальних мережах.
3. Протидія дезінформації на платформі, де вона поширюється.
4. Посилення стійкості населення України до дезінформаційних впливів та розвиток відповідального медіаспоживання.

Практичне заняття – 2 год.

План:

Робота із практичними ситуаціями:

- ознаки фейків у TikTok, Instagram та Facebook: розбір прикладів фейків і пропаганди в соціальних мережах;
- походження Telegram та аналіз ймовірних загроз інформаційній безпеці;
- розбір фейків в YouTube й основних причин блокування відео і каналів.

Практичні завдання:

Завдання 1. Перелічіть по п'ять ключових ознак фейків у розрізі соціальних мереж:

- ***ознаки фейків у TikTok,***
- ***ознаки фейків в Instagram;***
- ***ознаки фейків у Facebook;***
- ***ознаки фейків у Telegram;***
- ***ознаки фейків в YouTube.***

Рекомендації щодо організації процесу виконання цього завдання:

1. Оберіть соціальні мережі для аналізу. Розпочніть із визначення кожної з п'яти соціальних мереж, зазначених у завданні (TikTok, Instagram, Facebook, Telegram, YouTube).

2. Дослідження кожної соціальної мережі:

Ознайомтесь із характерними особливостями кожної платформи. Наприклад, TikTok відомий короткими відео, Instagram – візуальним контентом, Facebook – текстами і статтями, Telegram – каналами для обміну новинами, YouTube – відеоматеріалами.

3. Визначте специфічні ознаки фейків для кожної платформи. Розгляньте, як фейки можуть поширюватися в кожній мережі (наприклад, у TikTok – маніпуляції з відео, в Instagram – фальшиві фотографії, в Telegram – анонімні канали без перевірених джерел).

TikTok: зверніть увагу на короткі відео, маніпуляції через звуки або ефекти.

Instagram: досліджуйте фото та тексти під постами, маніпулювання через хештеги.

Facebook: знайдіть ознаки фейків у новинах або статтях, що супроводжуються фальшивими посиланнями або застарілими даними.

Telegram: зверніть увагу на анонімність каналів, швидке поширення неперевіреної інформації.

YouTube: шукайте фальшиві відео або неправдиві заголовки.

4. Для кожної соціальної мережі визначте п'ять ключових ознак фейків. Приділіть увагу тому, чому саме ці ознаки є характерними для конкретної платформи.

5. Структура відповіді. Використовуйте підпункти для кожної соціальної мережі, щоб відповідь була чіткою і організованою. У кінці завдання коротко підсумуйте, чому важливо знати ознаки фейків і як це допомагає в боротьбі з дезінформацією.

Завдання 2. Наведіть один приклад фейку, який ви зустріли в одній із вищезазначених соціальних мереж.

Рекомендації щодо організації процесу виконання цього завдання:

1. Вибір прикладу фейку.

Виберіть соціальну мережу, яку ви добре знаєте, або яка, на вашу думку, містить найбільше фейків. Згадайте реальний випадок фейку, який ви зустрічали в обраній мережі. Це може бути конкретний пост, відео або навіть ціла кампанія.

2. Опис фейку.

Детально опишіть, що саме було неправдою у цьому випадку. Зазначте, які маніпуляції використовувалися, щоб переконати користувачів у фальшивій інформації.

Якщо фейк був добре продуманий, опишіть його елементи (наприклад, використання емоційного контенту, підроблені зображення або неперевірені джерела).

3. Перевірка інформації.

Для підтвердження вашого прикладу надайте доказ, що фейк був спростований (стаття, повідомлення з офіційного джерела або аналіз фактів).

4. Структура відповіді.

Опис фейку має бути лаконічним, але деталізованим. Вкажіть дату, джерело та основні моменти маніпуляцій. Підсумуйте, як цей фейк міг вплинути на громадську думку та чому важливо вміти розпізнавати такі повідомлення.

Під час виконання завдання звертайте увагу на актуальні приклади фейків. Якщо маєте доступ до соціальних мереж, перегляньте останні новини або пости, які викликали сумніви.

Важливо використовувати реальні приклади, щоб продемонструвати конкретні ознаки фейків замість абстрактних пояснень.

Рекомендована література:

1. Лопатченко І. М., Помаза-Пономатерко А. Л., Батир Ю. Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. *Вісник національного університету цивільного захисту України*. 2024. № 1 (20). С. 14-24. URL : <http://repositsc.nuczu.edu.ua/bitstream/123456789/20308/1/2Lopatchenko.pdf>.

2. Мороз О. Нація овочів? Як інформація змінює мислення і поведінку українців. К. : Yakaboo Publishing, 2020. 288 с.

3. Польовий М., Стеблина Н., Болган В., Пархітько О. Ворожі інформаційні операції: нові виміри, нові виклики, нові медіа: навч.-практ. посібник. Одеса : ІзбірКом, 2021. 176 с.

4. Як захиститися від фейків і дезінформації: освітній серіал. *Дія: Освіта*. URL : <https://osvita.diia.gov.ua/courses/how-to-protect-yourself-from-fakes-and-disinformation>.

ТЕМА 5. ІНСТРУМЕНТИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ДЕСТРУКТИВНИМ КОМУНІКАЦІЙНИМ КАМΠΑНИЯМ В ПУБЛІЧНОМУ ПРОСТОРІ

Зміст теми:

Основні інструменти протидії дезінформації деструктивним комунікаційним кампаніям. Пеналізація та блокування дезінформації в інтернеті у світі. Інституційний вимір протидії дезінформації. Законодавча протидія поширенню дезінформації в Україні. Інтервенції для зниження впливу дезінформації на політичні переконання громадян: закордонний досвід для України.

Семінарське заняття – 2 год.

План:

1. Інституційний вимір протидії дезінформації.
2. Законодавча протидія поширенню дезінформації в Україні.
3. Інтервенції для зниження впливу дезінформації на політичні переконання громадян.

Практичне заняття – 2 год.

План:

Аналіз та оцінювання ефективності протидії російській дезінформації в Україні в умовах повномасштабної війни.

Практичне завдання:

Завдання. Пройдіть Національний тест з медіаграмотності за посиланням <https://filter.mcsc.gov.ua/start>.

Національний тест з медіаграмотності реалізовується національним проєктом з медіаграмотності «Фільтр» Міністерства культури та стратегічних комунікацій за підтримки ПРООН в Україні й фінансування уряду Японії, а також проєктом з медіаграмотності і когнітивної стійкості в Україні, що реалізується Zinc Network і фінансується урядом Великої Британії.

Рекомендації щодо організації процесу виконання цього завдання:

1. Перейдіть за посиланням та відкрийте Національний тест з медіаграмотності у вашому браузері.
2. Ознайомтесь із завданнями і намагайтесь відповідати на них на основі знань про медіаграмотність, здатність критично оцінювати інформацію.
3. Після проходження тесту ви отримаєте результат, який можна використовувати для самостійної оцінки вашого рівня медіаграмотності.
4. Після завершення тесту зверніть увагу на ваші помилки (якщо такі були), щоб покращити розуміння медіаграмотності.

Рекомендована література:

1. Азарова В. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни: практ. довід. К. : 7БЦ, 2023. 232 с.
2. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни: аналіт. звіт. К. : ГО «Український інститут медіа та комунікації», 2023. 66 с.
3. Трещов М. М., Наумик А. С. Цифровізація воюючої держави: необхідність та переваги. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. № 9.
4. Центр протидії дезінформації. URL : <https://cpd.gov.ua>.

ТЕМА 6. ДІЯЛЬНІСТЬ ТА ВЗАЄМОДІЯ ОРГАНІВ ВИКОНАВЧОЇ ВЛАДИ З ПИТАНЬ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Зміст теми:

Аналіз загроз та викликів інформаційній безпеці. Національні виклики та загрози інформаційній безпеці. Національна система стратегічних комунікацій. Складники плану дій зі стратегічних комунікацій. Українські інституції для протидії дезінформації. Фактчекінг у структурі стратегічних комунікацій. Стратегія інформаційної безпеки України. Механізми реалізації заходів щодо забезпечення інформаційної безпеки на державному рівні.

Семінарське заняття – 2 год.

План:

1. Українські інституції для протидії дезінформації.
2. Фактчекінг у структурі стратегічних комунікацій.
3. Стратегія інформаційної безпеки України.

Практичне заняття – 2 години

План:

1. Практичний вимір стратегічних комунікацій в умовах війни. Робота із кращими прикладами науково-практичної школи зі стратегічних комунікацій Національної академії Служби безпеки України.
2. Аналіз стану розвитку медіаграмотності в Україні: проєкти, ініціативи та виклики.

Практичні завдання:

Завдання 1. Зіграйте в гру «Bad News Game» за посиланням <https://www.getbadnews.com/ua>.

Довідково:

Що представляють собою «Погані новини»?

У «Поганих новинах» ви берете на себе роль розповсюджувача фейкових новин. Відмовтеся від етики й оберіть шлях, який створить з вас безпринципного медіамагната. Стежте за показниками своїх «прихильників» і «довіри»: ваше завдання полягає в тому, щоб отримати якомога більше підписників, поступово завойовуючи фальшивий авторитет новинного сайту. Але будьте обережні: ви програєте, якщо скажете явну брехню або розчаруєте своїх прихильників!

Як відбувається гра?

Мета гри полягає в тому, щоб викрити тактику й методи маніпулювання, які використовуються для введення людей в оману й залучення послідовників. «Погані новини» працюють як психологічна «вакцина» проти дезінформації: гра створює когнітивний опір поширеним формам маніпуляцій, з якими ви можете зіткнутися в мережі Інтернет.

Вчені, які працювали з нами над розробкою цієї гри, виявили, що вона покращує здатність людей виявляти методи маніпулювання в дописах соціальних мереж, підвищує їхню впевненість у виявленні таких прийомів і зменшує їх бажання ділитися маніпулятивним контентом з людьми у своїй мережі.

Для кого створена ця гра?

«Погані новини» створені для аудиторії віком від 14 років. У грі містяться незначні згадки про помірні форми насильства (зокрема, груба лексика у вигаданій соціальній мережі, хоча лайливі слова не використовуються), але немає контенту, який, імовірно, буде сприйнятий як шокуючий. Попри те, що гра містить посилання на події реального світу, її сценарії повністю вигадані. Було докладено чимало зусиль, щоб зробити гру максимально інклюзивною, аби нею могли насолоджуватися гравці з будь-яким попереднім досвідом.

Рекомендації щодо організації процесу виконання цього завдання:

1. Ознайомлення з інтерфейсом гри

Коли перейдете на гру, вона пояснить вам, що ви будете грати роль особи, яка навчається створювати фейкові новини та маніпулювати інформацією.

Існують кілька рівнів гри, де вам потрібно буде виконувати різні завдання, наприклад, створення фейкових новин, використання маніпуляцій або пропаганди.

2. Ігровий процес

Початковий етап. Гра починається з короткого вступу, в якому вам пояснюють правила гри. Вона запитує вас, чи готові ви маніпулювати новинами, щоб отримати вигоду або досягти своїх цілей.

Рольова частина. Ви будете виконувати різні завдання, створюючи фейкові новини за допомогою таких методів:

- використання емоцій – додавання драматичних елементів або викликаних емоцій, щоб зробити новину привабливою і легкою для поширення;
- маніпулювання фактами – використання частково правди, змішаної з вигадкою;
- залучення впливових осіб – використання популярних або авторитетних особистостей для підкріплення фейкових новин;
- вибір цільової аудиторії – визначення, яка група людей найбільше піддаватиметься маніпуляціям.

Завдання на кожному рівні. У грі ви будете отримувати завдання, де вам потрібно буде вибирати стратегії для поширення фейкової інформації. Наприклад: вибір слів для заголовків новин; створення та розповсюдження медіа-контенту, що підвищує емоційну привабливість новини; маніпулювання уявленнями людей через спотворення фактів.

Просування через соціальні мережі. Після того, як ви створите фейкові новини, вам буде потрібно поширити їх через різні канали (наприклад, через соціальні мережі). Це дозволить вам зрозуміти, як фейкові новини набирають популярності і які стратегії працюють найкраще.

3. Підсумки гри

Після проходження гри отримаєте результат, який відображає ваші навички у створенні та розповсюдженні фейкових новин. Гра також підсумовує, наскільки ефективно ви застосовували різні маніпуляції і які методи були найбільш успішними.

Гра надасть зворотний зв'язок, де побачите, що вдалося зробити добре, а що можна покращити. Цей зворотний зв'язок допоможе вам краще зрозуміти, як працюють фейкові новини та чому важливо бути критичним у споживанні інформації.

4. Важливі висновки

Після гри розгляньте її як навчальний інструмент для розуміння того, як можна маніпулювати інформацією та які фактори роблять новину привабливою для споживачів.

Пам'ятайте, що «Bad News Game» допомагає не тільки зрозуміти, як створюються фейкові новини, але і вчить вас, як їх розпізнавати в реальному житті.

Під час гри звертайте увагу на стратегії, які ви використовуєте, і на їх вплив на довіру до новин. Спробуйте уникати спрощених рішень, орієнтуючись на реальні медіа-процеси.

Розглядаючи свою поведінку в грі, намагайтеся перенести отримані знання на реальний контекст – як захиститися від фейків у соціальних мережах та в ЗМІ.

Гра є чудовим інструментом для розвитку критичного мислення щодо медіа та допомагає краще розуміти, як формуються маніпуляції з інформацією.

Рекомендована література:

1. Азарова В. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни: практ. довід. К. : 7БЦ, 2023. 232 с.

2. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни: аналіт. звіт. К. : ГО «Український інститут медіа та комунікації», 2023. 66 с.

3. Лопатченко І. М., Помаза-Пономатерко А. Л., Батир Ю. Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. *Вісник національного університету цивільного захисту України*. 2024. № 1 (20). С. 14-24. URL : <http://repositc.nuczu.edu.ua/bitstream/123456789/20308/1/2Lopatchenko.pdf>.

ТЕМА 7. АНАЛІЗ ПОДІЙ І ЯВИЩ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

Зміст теми:

Битва наративів у медіапросторі України: ретроспективний аналіз. Російська пропаганда після 24 лютого 2022 року: тренди та протидія. Проактивне реагування на кампанію з дискредитації українсько-польських відносин (із досвіду Центру протидії дезінформації Ради національної безпеки і оборони України).

Семінарське заняття – 2 год.

План:

1. Битва наративів у медіапросторі України.
2. Російська пропаганда після 24 лютого 2022 року: тренди та протидія.
3. Проактивне реагування на кампанію з дискредитації українсько-польських відносин.

Практичне заняття – 2 години

План:

1. Робота із практичними прикладами подій і явищ в сучасному інформаційному просторі України: розбір ситуацій.
2. Практичні рекомендації щодо наративних комунікацій в умовах російської агресії.

Практичні завдання:

Завдання 1. Подивитися освітній серіал «Як захиститися від фейків і дезінформації: базові навички з фактчекінгу та протидії дезінформації» на платформі Дія. Освіта за посиланням <https://osvita.diia.gov.ua/courses/how-to-protect-yourself-from-fakes-and-disinformation>.

Пройти фінальне тестування.

Довідково.

Як захиститися від фейків і дезінформації – це 10 серій, насичених знаннями з протидії фейкам і дезінформації, захисту особистих даних і порадами з безпеки в інтернеті. У форматі діалогу ведучий Святослав Гринчук разом з гостем-експертом обговорюють окремі теми з медіаграмотності. Освітній серіал надасть глядачам практичні навички медійної та інформаційної грамотності, які мають стати частиною їхнього життя в умовах повномасштабної війни, а також пояснить, як орієнтуватися в інформації довкола та розпізнавати дезінформацію й пропаганду.

Освітній серіал створено для платформи Дія.Освіта Міністерства цифрової трансформації в межах «Всеохопної інформаційно-просвітницької кампанії з протидії дезінформації», що впроваджується 1+1 media та Smart Angel у співпраці з експертними організаціями за фінансової підтримки Європейського Союзу. Його зміст є виключною відповідальністю редакції серіалу й не обов'язково відображає позицію ЄС.

Рекомендації щодо організації процесу виконання цього завдання:

1. Перехід на платформу Дія. Освіта

Відкрийте ваш веб-браузер (наприклад, Google Chrome, Mozilla Firefox, Safari). Перейдіть за посиланням: Освітній серіал «Як захиститися від фейків і дезінформації».

2. Ознайомлення з платформою

На сайті ви побачите сторінку курсу, яка містить опис навчального матеріалу. Ознайомтесь з інформацією про серіал, щоб зрозуміти, що саме вам буде потрібно вивчити. Вам може знадобитися зареєструватися або увійти через електронну пошту або в порталі Дія, щоб отримати доступ до курсу.

3. Перегляд серіалу

Натискайте на кнопку «Почати курс» або подібну, щоб розпочати перегляд серіалу. Серіал складається з кількох відео або модулів, в яких ви будете вивчати базові навички з фактчекінгу, визначення фейків і дезінформації. Дивіться кожен урок уважно, звертайте увагу на ключові поради і техніки для перевірки інформації. Під час перегляду серіалу у вас можуть виникнути питання або завдання для перевірки знань.

4. Завершення курсу

Після завершення курсу вам, ймовірно, буде запропоновано пройти тест або відповісти на запитання для оцінки ваших знань. Якщо є можливість, пройдіть тестування, щоб оцінити, наскільки добре ви засвоїли матеріал. Переконайтесь, що отримали сертифікат або підтвердження про завершення курсу.

5. Висновки

Після завершення серіалу подумайте про те, як отримані знання можна застосувати у реальному житті для розпізнавання фейків і дезінформації. Поділіться результатами з іншими, якщо потрібно, або використовуйте отримані знання для вдосконалення ваших навичок у перевірці фактів.

Цей курс допоможе вам краще зрозуміти механізми поширення дезінформації і навчитись ефективно протидіяти їй.

Рекомендована література:

1. Азарова В. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни: практ. довід. К. : 7БЦ, 2023. 232 с.

2. Онлайн-медіа, що стали найякіснішими: Білий список другого півріччя 2023. *Інститут масової інформації*. URL : <https://imi.org.ua/monitorings/onlajn-media-shho-staly-najyakisnishymy-bilyj-spysok-drugogo-pivrichchya-2023-i55817>.

3. Список безпечних каналів отримання інформації. *Центр протидії дезінформації*. URL : <https://cpd.gov.ua/reports/spysok-bezpechnyh-kanaliv-otrymannya-informacziyi>.

4. Центр протидії дезінформації. URL : <https://cpd.gov.ua>.

ТЕМА 8. ДЕРЖАВНА ПОЛІТИКА КІБЕРБЕЗПЕКИ

Зміст теми:

Поняття «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «кіберзлочин», «кіберінцидент», «кіберпростір», «кібертероризм», «критична інформаційна інфраструктура». Сутність проблеми кібербезпеки: переваги та загрози цифровізації суспільної діяльності. Суб'єкти забезпечення кібербезпеки. Принципи забезпечення кібербезпеки. Основні напрями забезпечення кібербезпеки. Національна система кібербезпеки. Основні заходи протидії кіберзагрозам у контексті забезпечення кібербезпеки держави.

Семінарське заняття – 2 год.

План:

1. Принципи забезпечення кібербезпеки.
2. Основні напрями забезпечення кібербезпеки.
3. Національна система кібербезпеки.
4. Основні заходи протидії кіберзагрозам у контексті забезпечення кібербезпеки держави.

Практичне заняття – 2 год.

План:

1. Етапи забезпечення ефективності системи управління розвитком кібербезпеки.
2. Вебпортал органу влади як об'єкт кібератаки: правові аспекти.

Практичні завдання:

Завдання 1. Розробка сценарію кібератаки на вебпортал органу влади з урахуванням правових аспектів і заходів захисту.

Розробити детальний сценарій кібератаки на вебпортал органу влади (наприклад, портал для подачі документів чи доступу до державних послуг), зокрема:

- проаналізувати потенційні вразливості порталу;
- створити можливі сценарії кібератак (наприклад, SQL-ін'єкція, DDoS-атака, фішинг);
- оцінити правові наслідки таких атак для органу влади, його користувачів та третіх осіб;
- запропонувати заходи для захисту та реагування на інциденти (з точки зору як кібербезпеки, так і юридичних аспектів).

Рекомендації щодо організації процесу виконання цього завдання:

1. Аналіз вебпорталу.

Оцінка типових вразливостей вебсайтів органів влади.

Аналіз ризиків, що виникають через відсутність захисту або слабкі місця системи (наприклад, незахищені форми введення даних або недостатній контроль доступу).

2. Розробка сценаріїв атак.

Вибрати одну чи кілька форм атак і детально описати, як би вони могли реалізувати такі атаки на порталі органу влади.

3. Оцінка можливих наслідків кожної атаки: для користувачів, органу влади та суспільства.

Аналіз правових наслідків:

– визначити правові наслідки для органів влади та користувачів у разі успішної атаки;

– з'ясувати, які законодавчі норми можуть бути порушені внаслідок таких інцидентів (наприклад, порушення захисту персональних даних).

4. Розробка заходів захисту.

Оцінка існуючих заходів кібербезпеки для запобігання атакам.

Розробка рекомендацій щодо покращення безпеки (наприклад, впровадження багаторівневого захисту, аудит системи безпеки, регулярні тести на вразливості).

5. Юридична відповідальність.

Обговорення юридичних наслідків для органів влади у разі недотримання стандартів кібербезпеки; оцінка можливих штрафів або санкцій для органів влади та осіб, відповідальних за кібербезпеку.

6. Підготувати презентацію для захисту свого сценарію кібератаки та заходів захисту.

Це завдання дозволяє не тільки освоїти теоретичні аспекти кібербезпеки та права, але й розвивати практичні навички у вирішенні реальних проблем, що виникають у сфері захисту інформаційних систем органів влади.

Рекомендована література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19>.

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: указ Президента України; Стратегія від 28.12.2021 р. № 685/2021. URL : <https://zakon.rada.gov.ua/laws/show/685/2021>.

3. Про Стратегію комунікації з питань євроатлантичної інтеграції України на період до 2025 року: указ Президента від 11.08.2021 р. № 348/2021. URL : <https://zakon.rada.gov.ua/laws/show/348/2021>.

4. Матвеева О. Ю., Мунько А. Ю. Упровадження концепції розумного міста у процеси цифрової трансформації України заради сталого розвитку. *Науковий вісник: державне управління*. 2023. № 1(13). С. 138-162.

5. Трещов М. М. Імплементация Common Reporting Standard задля забезпечення інституційної спроможності місцевих органів публічної влади. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. № 15.

6. Трещов М. М., Наумик А. С. Цифровізація воюючої держави: необхідність та переваги. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. № 9.

7. Трещов М. М., Хохба О. Т. Удосконалення методології смартизації управління розвитком територій. *Науковий вісник: державне управління*. 2023. № 1(13). С. 178-194.

8. Kryshtanovych, M., Storozhev, R., Malyshev, K., Munko, A., Khokhba, O. (2022). State Management of the Development of National Cybersecurity Systems. *International Journal of Computer Science and Network Security*, 22(5), 11-16.

ПИТАННЯ ТА ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою інформаційна гігієна?
2. Які основні принципи інформаційної гігієни?
3. Як дезінформація впливає на суспільство?
4. Що представляють собою фейкові новини?
5. Які ознаки можуть вказувати на дезінформацію в новинах?
6. Які основні джерела поширення дезінформації?
7. Як перевірити правдивість інформації в мережі Інтернет?
8. Охарактеризуйте поняття цифрової грамотності і її значення для людини, суспільства і держави.
9. Як використовувати перевірку фактів для боротьби з дезінформацією?
10. Які інструменти можна використовувати для перевірки інформації?
11. Що являє собою маніпулювання фактами?
12. Які техніки маніпулювання можуть бути використані в публічному просторі?
13. Як соціальні мережі сприяють поширенню дезінформації?
14. Як захистити себе від маніпуляцій у медіапросторі?
15. Які етичні проблеми виникають при використанні інформації в публічному просторі?
16. Як використовувати критичне мислення для оцінки інформації?
17. Які принципи працюють при аналізі медіаповідомлень?
18. Як розпізнати пропаганду у засобах масової інформації?
19. Охарактеризуйте так званий «груповий ефект» в контексті медіапсихології.
20. Як фактчекінг допомагає боротися з дезінформацією?
21. Яка роль алгоритмів у поширенні фейкових новин?
22. Які ознаки вказують на пропагандистський контент?
23. Що представляє собою «групове мислення» в медіаполітиці?
24. Як уникнути потрапляння в «інформаційні пастки» в мережі Інтернет?
25. Як розпізнати мову ненависті та екстремізм в інформаційних матеріалах?
26. Як політичні сили можуть використовувати дезінформацію?
27. Охарактеризуйте інформаційні війни та наведіть їх ознаки.
28. Як визначити надійність джерела інформації?
29. Як медіа можуть сприяти боротьбі з дезінформацією?
30. Які стратегії протидії дезінформації застосовують держави?
31. Як правильно використовувати ресурси для перевірки новин?
32. Як визначити, чи є джерело новин зацікавленим у маніпуляціях?
33. Опишіть найбільш поширені техніки створення фейкових новин.
34. Як працює емоційний вплив у дезінформаційних кампаніях?
35. Наведіть алгоритм аналізу графіки та відео для визначення фейкових матеріалів.

36. Які фактори впливають на сприйняття інформації у користувачів соціальних мереж?

37. Як уникнути поширення дезінформації серед близьких та друзів?

38. Які правові механізми боротьби з дезінформацією існують в Україні?

39. Охарактеризуйте міжнародні стандарти протидії дезінформації.

40. Як ефективно навчати населення критичному мисленню в контексті медіа?

41. Як фейкові новини можуть впливати на виборчі процеси?

42. Як використовуються «інфографіка» та «меми» для поширення маніпуляцій?

43. Яка роль громадянського суспільства у боротьбі з дезінформацією?

44. Як визначити надійність вебсайту як джерела інформації?

45. Що представляють собою «хибні факти» і як з ними боротися?

46. Як виявити «зміщення» в поданні фактів у новинах?

47. Як вчитися розпізнавати маніпуляції в соціальних мережах?

48. Які є стратегії для покращення інформаційної безпеки громадян?

49. Як держави повинні реагувати на використання дезінформації іншими країнами?

50. Як за допомогою контексту можна визначити, чи є інформація достовірною?

51. Охарактеризуйте поняття «хибного відчуття консенсусу» у контексті інформаційної маніпуляції.

52. Які засоби можуть бути використані для виявлення фотошоплених зображень?

53. Які методи використовуються для поширення «конспірологічних теорій» в Інтернеті?

54. Як використовувати ментальні «схеми» для визначення правдивості інформації?

55. Які критерії використовуються для оцінки надійності медіа?

56. Як покращити свою інформаційну гігієну при роботі з новинами на мобільних пристроях?

57. Які інструменти можна використовувати для виявлення змін у текстах або фотографіях?

58. Як алгоритми в соціальних мережах сприяють розповсюдженню поляризації в суспільстві?

59. Як виявити та уникнути «систематичної дезінформації» з боку державних органів?

60. Опишіть поняття «інформаційних ехо-камер» і їх впливу на сприйняття новин.

61. Які причини викликають феномен «згідних підтверджень» в інформаційних процесах?

62. Як соціальні мережі маніпулюють емоціями своїх користувачів для поширення новин?

63. Як відрізнити науково обґрунтовані дані від маніпуляцій в медіа?
64. Які фактори можуть свідчити про організовану кампанію з дезінформації в мережі Інтернет?
65. Як здійснювати аудит джерел інформації в медіа?
66. Як можна захистити свою приватність при взаємодії з цифровими медіа?
67. Розкрийте зміст поняття «література з компіляцією». Як її розпізнати?
68. Як фейкові новини впливають на довіру до традиційних медіа?
69. Як при перевірці новини відрізнити достовірні факти та інтерпретації?
70. Які психологічні ефекти виникають від частого споживання дезінформації?
71. Як змінити сприйняття інформації за допомогою маніпуляцій через текст?
72. Як працює інформаційний «асиметричний потік» між різними типами медіа?
73. Як можна виявити заангажованість журналістів у висвітленні подій?
74. Як фейкові новини можуть створювати кризу довіри в суспільстві?
75. Які ролі можуть виконувати «тролі» в мережі Інтернет для поширення дезінформації?
76. Як відрізнити сатиричні матеріали від серйозних новин?
77. Які стратегії використовуються для створення вигідного для когось «інформаційного шуму»?
78. Як інтернет-платформи можуть сприяти боротьбі з дезінформацією на своєму рівні?
79. Які існують механізми для боротьби з автоматичними ботами, що поширюють фейки?
80. Опишіть алгоритм проведення аналізу медіа-контенту з точки зору його соціальної значущості.
81. Назвіть провідні міжнародні організації, які працюють над питанням протидії дезінформації, та коротко опишіть їх діяльність.
82. Як виявити упередженість у новинах щодо певних соціальних груп?
83. Розкрийте поняття «освітні кампанії» проти дезінформації та опишіть процес їх використання.
84. Як використовувати наративи для боротьби з фейковими новинами?
85. Яку роль відіграє співпраця між урядами та медіа у боротьбі з дезінформацією?
86. Як з'ясувати чи є матеріал частиною рекламної кампанії, прихованої під новину?
87. Які техніки пропаганди застосовуються в кризових ситуаціях?
88. Як цифрові технології змінюють спосіб сприйняття політичних новин?
89. Як виявити фактографічні помилки в текстах новин?
90. Які юридичні наслідки можуть виникнути за поширення дезінформації через медіа?

91. Як соціальні мережі можуть використовувати алгоритми для обмеження дезінформації?
92. Які є наукові підходи до аналізу фейкових новин?
93. Як можна оцінити достовірність відеоматеріалів, що поширюються в Інтернеті?
94. Як ідентифікувати фейкові акаунти у соціальних мережах?
95. Як критичне мислення допомагає розпізнавати маніпуляції у новинах?
96. Як розпізнати дезінформацію на основі медіаформату?
97. Як соціальні та психологічні фактори впливають на поширення фейкових новин?
98. Як покращити медіаосвіту серед молоді для боротьби з дезінформацією?
99. Як розрізняти офіційні та неофіційні джерела в публічному просторі?
100. Яким чином технології штучного інтелекту можуть бути використані для виявлення та боротьби з дезінформацією?

Навчальне видання

Трещов Мирослав Миколайович

**МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДЛЯ ПРОВЕДЕННЯ СЕМІНАРСЬКИХ ТА ПРАКТИЧНИХ ЗАНЯТЬ
З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА ГІГІЄНА
ТА ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ»**

Редактор, оригінал-макет – *А. В. Самотуга*
Коректор *М. С. Касян*

Підп. до друку 10.06.2025. Формат 60x84/16. Друк – цифровий.
Гарнітура – Times New Roman. Ум.-друк. арк. 1,63. Обл.-вид. арк. 1,75.

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до державного реєстру видавців ДК № 8112 від 13.06.2024