

Інформаційна безпека населення під час виникнення надзвичайних ситуацій

Мета:

Сформувати розуміння важливості інформаційної безпеки під час надзвичайних ситуацій та надати практичні поради щодо критичного сприйняття інформації.

▶ Завдання:

- ▶ Розкрити сутність та значення інформації у контексті цивільного захисту.
- ▶ Визначити основні загрози інформаційній безпеці під час війни та кризових ситуацій.
- ▶ Пояснити, як розпізнавати фейки, дезінформацію та маніпуляції.
- ▶ Ознайомити з методами захисту від небезпек соцмереж, зокрема вербування та психологічного впливу.
- ▶ Показати, як інформаційний потік впливає на психологічний стан дітей і дорослих.
- ▶ Надати практичні рекомендації щодо основ інформаційної безпеки.

РОЗДІЛ 1. СУТНІСТЬ ТА РОЛЬ ІНФОРМАЦІЇ В КОНТЕКСТІ ЦИВІЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ

- ▶ Інформацією вважають:
- ▶ сукупність даних, що мають значення, і метою яких є розширення знань, інформування чи внесок ідей щодо певної теми;
- ▶ це сукупність різних повідомлень про зміни, які проходять в системі й навколишньому середовищі.



В Цивільному Кодексі у ст. 200 знаходимо визначення інформації як *документованих або публічно оголошених відомостей про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі.*

- ▶ Основою будь-якого інформаційного протистояння є інформаційний процес.



- ▶ **Інформаційна війна** (англ. *information warfare*) — викладення інформації у спосіб, який формує у суспільстві чи групі людей потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів щодо окремих питань на користь організатора інформаційної пропаганди.



РОЗДІЛ 2. ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ВІЙНИ

- ▶ Інформаційну безпеку України можна інтерпретувати як сукупність життєво важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства

**Інформаційна
безпека**



Складові інформаційної безпеки:

Технічна
безпека

Медійна
грамотність

Психологічна
стійкість

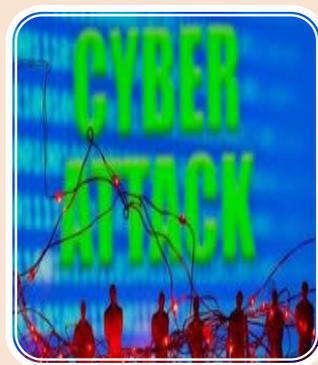
інформац
ійна
безпека
особистос
ті

Види
діяльності
за сферою
застосуван
ня

інформац
ійна
безпека
держави

інформац
ійна
безпека
організац
ії

Основні інформаційні загрози



Дезінформація :

- поширення неправдивої інформації для введення в оману.

Пропаганда:

- систематичне нав'язування ідей для впливу на думки та поведінку.

Фейкові новини:

- сфабриковані повідомлення, що маскуються під реальні новини.

Кібернапади:

- атаки на інформаційні системи для дестабілізації та отримання даних.

Соціальна інженерія:

- маніпуляція людьми для отримання конфіденційної інформації.

Пропаганда, дезінформація, фейки: як їх розпізнавати

Перевірка джерела:
оцінюйте надійність та репутацію джерела інформації.



Аналіз заголовків:
уникайте сенсаційних та емоційно забарвлених заголовків.



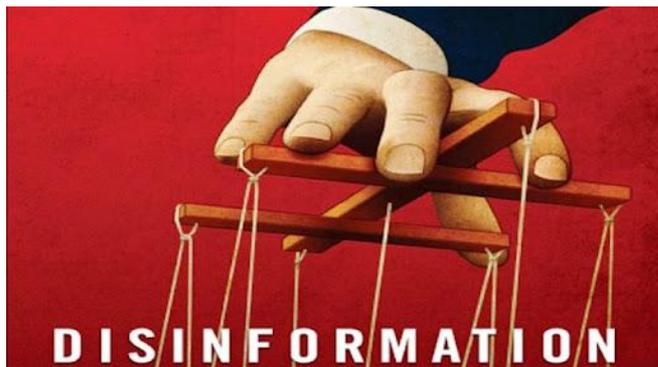
Перехресна перевірка:
звіряйте інформацію з декількох незалежних джерел.



Перевірка дат: звертайте увагу на актуальність та час публікації.



Оцінка емоційного впливу: будьте обережні з матеріалами, що викликають сильні емоції.



Як медіа можуть впливати на емоційний стан людей?

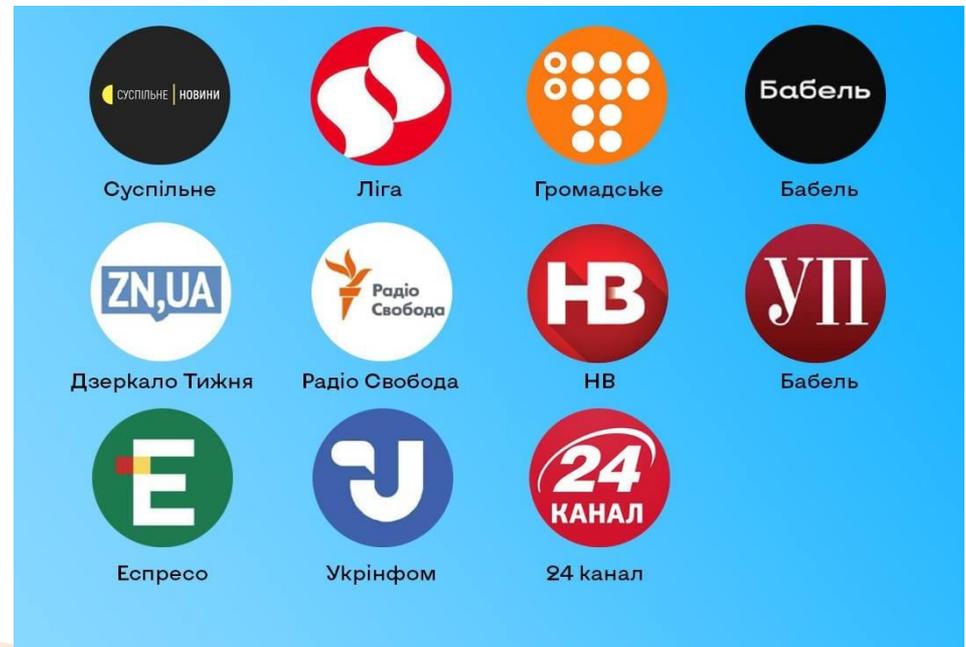
- ▶ **Емоційне навантаження:** постійний потік негативних новин може викликати тривогу та стрес.
- ▶ **Формування світогляду:** медіа впливають на сприйняття реальності та особисті переконання.
- ▶ **Ефект повторення:** часте повторення інформації підсилює її вплив на свідомість.
- ▶ **Соціальне порівняння:** соцмережі можуть сприяти відчуттю неповноцінності через ідеалізовані образи.
- ▶ **Інформаційна перевантаженість:** надлишок інформації може призвести до емоційного виснаження.

Психологічна стійкість як частина інформаційної безпеки

- ▶ **Визначення психологічної стійкості:**
 - Здатність особистості протистояти стресовим ситуаціям та швидко відновлюватися після них.
- ▶ **Роль у контексті інформаційної безпеки:**
 - Захист від маніпуляцій та дезінформації.
 - Підтримка критичного мислення.
- ▶ **Методи розвитку психологічної стійкості:**
 - Навчання критичному аналізу інформації.
 - Розвиток емоційної інтелігентності.
 - Практика стресостійкості.

РОЗДІЛ 3: ДЖЕРЕЛА ІНФОРМАЦІЇ ТА РІВЕНЬ ЇХНЬОЇ ДОВІРИ

	Офіційні	Неофіційні
ЛЮДИ	Посадові особи Прес-служби Представники партій на НУО Директори компаній	Свідки «Колишні» Постраждаді Інсайдери
ДОКУМЕНТИ	Законодавство Архіви Статистика Відповіді на інформаційні запити	Листи Щоденники Особисті архіви Розписки



Ризики соцмереж

Основні загрози:

- Вербування в екстремістські організації
- Шантаж та вимагання
- Кібербулінг та онлайн-цькування



Методи захисту:

- Налаштування конфіденційності акаунтів
- Обережність при спілкуванні з незнайомцями
- Використання двофакторної автентифікації



- Емоційно забарвлені заголовки
- Відсутність посилань на офіційні джерела
- Непереверені або анонімні автори

Ознаки
маніпулятивної
інформації:



- Перевірка інформації в декількох джерелах
- Критичне мислення та аналіз контенту
- Використання офіційних та надійних джерел інформації

Стратегії
захисту:



Методи фактчекінгу

Перевірка джерела

Перехресна перевірка

Аналіз контенту

Використання спеціалізованих сервісів

VoxChecked



АРСЕНІЙ ЯЦЕНЮК
ПРО СТІНУ НА КОРДОНІ З РОСІЄЮ

”

16 лютого 2016:
"Ми виконали близько 20% необхідних робіт"

19 вересня 2016:
"Через недофінансування Стіна побудована на 12%"

“

НЕПОСЛІДОВНІСТЬ

VoxChecked



ПЕТРО ПОРОШЕНКО
ПРО ТРАНШ МВФ

"Вперше в історії відносин між Україною і МВФ наша країна отримує 3й транш допомоги в рамках однієї програми співробітництва"

В 2009 році Україна також отримувала третій транш в рамках однієї програми з МВФ

НЕПРАВДА

Кроки перевірки новин:

Оцінка джерела

Перевірка дати публікації

Аналіз заголовка та змісту

Пошук підтвердження в інших джерелах

Використання фактчекінгових ресурсів



Роль державних структур у забезпеченні достовірної інформації



Головнокомандувач
ЗСУ



Служба безпеки
України



Державна
прикордонна
служба

Ключові
державні
органи:

- Державна служба України з надзвичайних ситуацій (ДСНС)
- Міністерство внутрішніх справ України (МВС)
- Державна прикордонна служба України

Основні
функції:

- Оперативне інформування населення про надзвичайні ситуації
- Надання офіційних рекомендацій та інструкцій
- Співпраця з медіа для поширення достовірної інформації



Державна служба
України
з надзвичайних
ситуацій



Міністерство
внутрішніх
справ України



Державна служба
спеціального зв'язку
та захисту інформації
України

РОЗДІЛ 4. ПСИХОЛОГІЧНИЙ ТА ЕМОЦІЙНИЙ ВПЛИВ ІНФОРМАЦІЇ НА ДІТЕЙ ТА ДОРΟΣЛИХ

- ▶ **Інформаційне перенасичення:**
 - Постійний потік новин може призвести до відчуття втоми та тривоги.
 - Зниження концентрації та уваги.
 - Погіршення пам'яті та розуміння.
- ▶ **Психосоматичні СИМПТОМИ:**
 - Надмірна перевірка інформації.
 - Втрата інтересу або апатія.



- Встановлення чітких часових рамок для перегляду новин.

Обмеження часу
споживання
новин:



- Аналіз джерел інформації та їх достовірності.

Критичне
мислення:



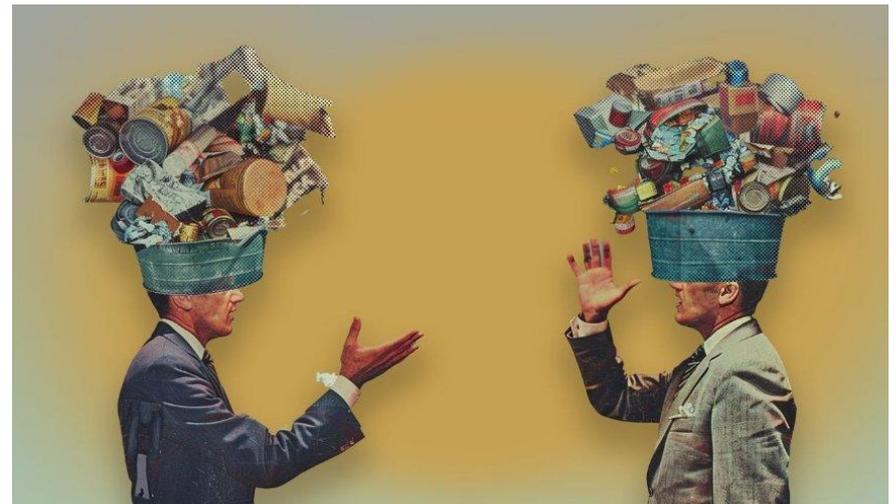
- Зайняття хобі,
фізичними
вправами,
медитацією.

Розвиток
ПОЗИТИВНИХ
ЗВИЧОК:



Інформаційна гігієна

- ▶ **Вибір надійних джерел:**
 - Довіра лише перевіреним та офіційним джерелам інформації.
- ▶ **Дозування інформаційного потоку:**
 - Обмеження кількості споживаної інформації щодня.
- ▶ **Відпочинок від цифрових пристроїв:**
 - Регулярні перерви від гаджетів та соціальних мереж.



Роль соціального працівника у підтримці емоційного стану клієнтів



Підходи до навчання (при роботі з дітьми):

- Використання інтерактивних методів.
- Обговорення реальних прикладів.

Основні теми для обговорення (при роботі з літніми людьми):

- Розпізнавання фейкових новин.
- Безпека в соціальних мережах.
- Захист особистих даних.

Рекомендації для соціальних працівників:

- Створення довірчої атмосфери.
- Заохочення критичного мислення.
- Регулярне оновлення знань про сучасні інформаційні загрози.

Діалог з клієнтами: як пояснити ризики соцмереж?

- ▶ *Ризики соцмереж: кібербулінг, витік особистих даних, вплив стереотипів.*
- ▶ Важливість відкритих розмов із дітьми про онлайн-безпеку.
- ▶ Розробка разом із дітьми правил безпеки в інтернеті.
- ▶ Акцент на конфіденційність і обережність при взаємодії з незнайомцями.

Критичне мислення для
розпізнавання
маніпуляцій.

Перевірка джерел: хто
написав, де факти, які
альтернативні думки.

**Як розрізнати
правдиву та
маніпулятивну
інформацію?**

Аналіз новин,
порівняння джерел
інформації.

Увага до емоційно
забарвлених матеріалів
і маніпуляцій.

Практичні поради щодо безпеки в інтернеті

- ▶ Використання складних паролів та налаштування безпеки.
- ▶ Батькам — сімейні налаштування безпеки.
- ▶ «Цифрова етика»: розрізнення публічної і приватної інформації.
- ▶ Заборона на публікацію особистих даних, фото та відео без згоди.



*Довідник
Цифрового
етикету для дітей
(за QR-кодом)*

Розділ 5. Корисна інформація та алгоритми дій під час НС

- ▶ Лише офіційні джерела інформації.
- ▶ Використання інструкцій, що підтверджені державними органами.
- ▶ Важливість своєчасного отримання інформації.
- ▶ Перевірка джерела перед виконанням інструкцій.





Офіційні
урядові
ресурси:
сайти,
соцмережі.



Місцеві
органи
влади та
служби
екстреної
допомоги.



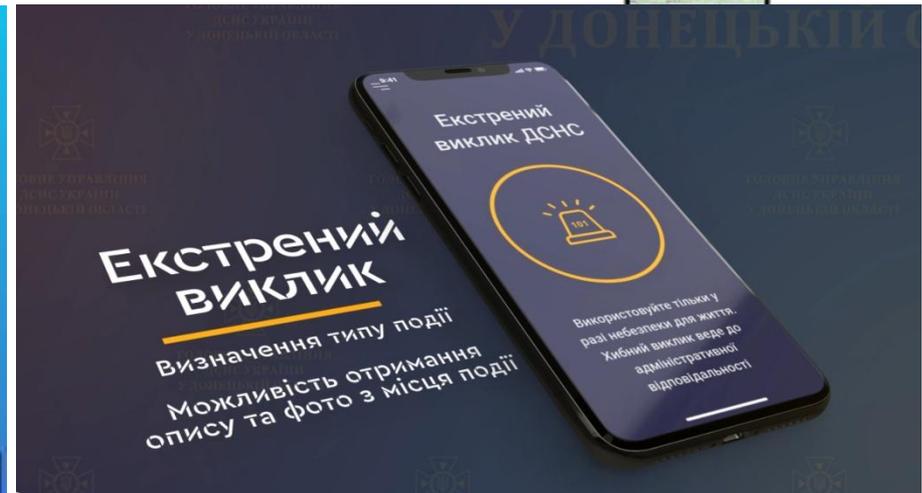
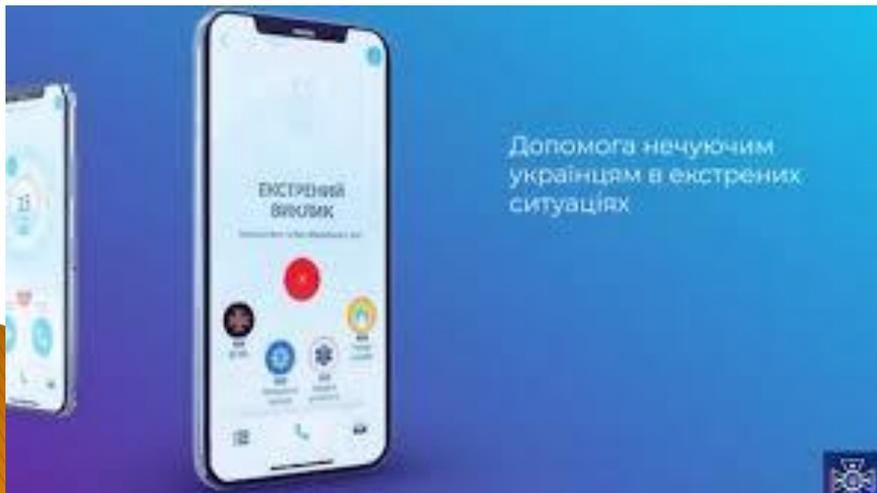
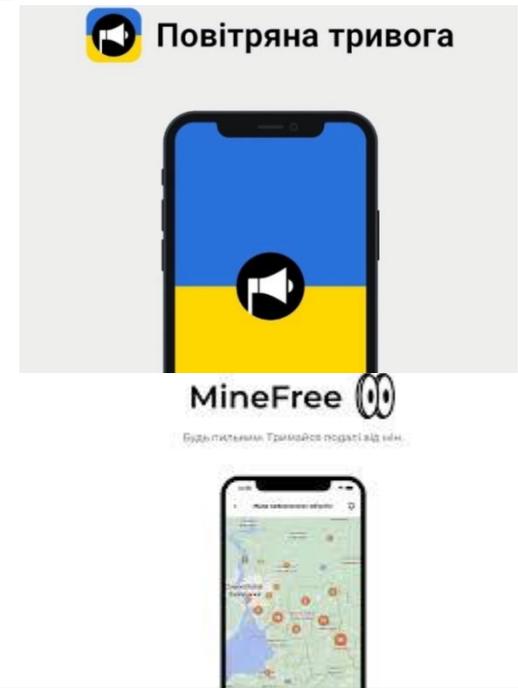
Важливість
перевірки
джерела
перед
довірою.



Застосування
перевірених
мобільних
додатків.

Роль мобільних застосунків

- ▶ Месенджери як швидкий засіб комунікації.
- ▶ Спеціалізовані додатки для поширення інструкцій у НС.
- ▶ Налаштування сповіщень для оперативності.



Алгоритм дій для соціальних працівників: як правильно передавати інформацію клієнтам?

- ▶ Використання простих та чітких інструкцій.
- ▶ Пояснення важливості дотримання правил безпеки.
- ▶ Перевірка інформації перед її передачею.
- ▶ Спокійне та впевнене донесення інформації.



Висновки

- ▶ Інформаційна безпека є ключовою для захисту в умовах надзвичайних ситуацій. Важливо критично оцінювати джерела інформації, довіряти лише перевіреним каналам та навчати дітей розрізняти правду від маніпуляцій. Вчителі та батьки повинні бути прикладом інформаційної відповідальності, навчаючи молодь самостійно мислити та перевіряти факти для забезпечення безпеки та адаптації до змін.