МАЙСТЕРНЯ ПОЛІТИК
DOVIDKA.INFO

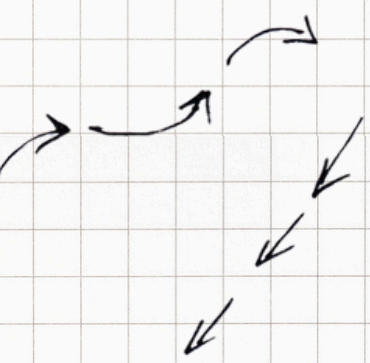
Бути готовим — означає бути вільним

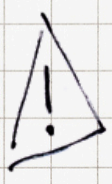
11 КЛАС

ПОСІБНИК ЗІ СЦЕНАРІЯМИ УРОКІВ ОНОВЛЕНОГО ПРЕДМЕТА *“ЗАХИСТ УКРАЇНИ”*

MARCH

ТРИВОГА → УКРИТТЯ





Схвалено до використання в освітньому процесі

Над сценаріями працювали:

Ганна Молодичук
тренерка та супервізорка предмета «Захист України», вчителька Соколівського опорного ліцею Жашківської міської ради Уманського району Черкаської області.

Михайло Борисевич
тренер та супервізор предмета «Захист України», вчитель «Міського юридичного ліцею наукового спрямування при Університеті митної справи та фінансів» Дніпровської міської ради.

Михайло Купчин
ветеран, тренер предмета «Захист України», керівник гуртка «Бойові Мурахи».

Катерина Сухоручко
тренерка та супервізорка предмета «Захист України», вчителька комунального закладу «Ліцей «Лідер» Кропивницької міської ради».

Тарас Пристацький
військовослужбовець, тренер предмета «Захист України», колишній вчитель ЦНПВ у Львові, а нині молодший сержант 13 БрОП НГУ «Хартія».

Гриф надано 30.12.2025, протокол засідання №17, №БО-0550-25

Передмова

Колеги, перед вами — збірка сценаріїв уроків, розроблена нашою командою відповідно до оновленої Модельної навчальної програми «Захист України. Інтегрований курс».
Підходячи до розробки кожного уроку, ми ставили собі ключове питання: «Що має на ньому відбутись з учнем та ученицею?». Ми прагнули, щоб підлітки не просто засвоїли інформацію, а відчули інтерес, набули реальних, життєво необхідних навичок і зрозуміли глибинний сенс своєї ролі як громадяни та громадянки України.
Саме тому ми зробили все можливе, щоб наші уроки були цікавими для підлітків: максимально мінімізували теорію і зосередилися на практичних відпрацюваннях у форматі інтенсивних тренінгових занять.

У цій збірці ви знайдете:

- Календарно-тематичне планування.
- Чіткі покрокові плани уроків для роботи в Осередках.
- Цікаві ігри та вправи для кращого засвоєння матеріалу.
- Презентації до кожного сценарію.

Ми пропонуємо викладати за двома підходами:

- **послідовний підхід:** дотримуючись логіки та структури модельної навчальної програми.
- **комбінований підхід:** об'єднуючи в одному тренінговому занятті теми різних модулів. Це дозволить учням та ученицям упродовж 4 або 8 уроків в Осередку знайомитись з різними модулями програми.

Для ми пропонуємо два різних підходи до фомування календарно-тематичного плану: послідовний за переліком модулів в МНП та комбінований. Вибір за вами — адже лише ви, як педагоги, найкраще знаєте своїх учнів та учениць, розумієте їхній освітній запит та освітні потреби.
Ми розуміємо, наскільки напруженою є праця вчителя сьогодні. Наша мета — не додати вам роботи, а навпаки, забрати рутину і спростити підготовку. Ми сподіваємося, що отримавши ці готові, продумані та гнучкі сценарії, ви зможете звільнити свій час для найважливішого: для живого спілкування з учнями та ученицями, їхньої підтримки та адаптації матеріалу під потреби вашого класу. Дякуємо вам за щоденну відданість і за те, що робите цей важливий предмет кращим!

Ми прагнемо, щоб наші матеріали були максимально корисними та ефективними. Саме тому ми готові чути ваш зворотний зв’язок та вдосконалювати наші напрацювання разом з вами!

Свої зауваження, ідеї чи пропозиції ви можете надіслати нам:

- На електронну пошту: **defenseofukraineteam@gmail.com**
- Або анонімно, заповнивши коротку форму за посиланням: https://forms.gle/Lye6vSFbubGQ5d596

Ваша думка надзвичайно важлива для нас. Дякуємо, що ви з нами!

ЗМІСТ

Посилання на презентацію до тренінгу.

Психоемоційна безпека та організація простору

- **Оцінка емоційного фону класу:** на початку заняття запропонуйте учням та ученицям коротко поділитися настроєм («Одним словом: як ви почуваєтеся сьогодні?»). Зверніть увагу на тих, хто мовчить або виглядає стривожено, щоб за потреби надати індивідуальну підтримку.

- **Вправа на заспокоєння (2–3 хв):** глибоке дихання. Попросіть учнів та учениць повільно вдихнути, подумки рахуючи до 4-х, затримати дихання — порахувати до 4-х, зробити видих — порахувати до 4-х, знову затримати дихання — також порахувати до 4-х. Повторіть 2–3 рази.

- **Коротка вправа на мовчання: запропонуйте учням та ученицям заплющити очі та зосередитися на власних думках і відчуттях, «відпустити» зайві емоції.**

- **Правила безпечного спілкування** (проговоріть їх на початку уроку): Висловлюватися по черзі, не перебиваючи;
  Поважати право інших на іншу думку, навіть якщо вона не збігається з вашою;
  Уникати жорстких політичних суджень і тримати фокус на фактах та емоціях.

- **Індикатори стресу, на які варто звернути увагу.**
  Емоційні: занепокоєння, плач, дратівливість, апатія, надмірна збудженість.
  Фізичні: прискорене дихання, тремтіння рук, м’язове напруження, почервоніння.
  Поведінкові: уникнення контакту, зацикленість на темі, агресія, ізоляція.

- **Дія вчителя чи вчительки при виявленні ознак стресу:** зробити паузу, м’яко звернутися до учня чи учениці, запропонувати вийти на мить або перемикнутися на легшу вправу, забезпечити конфіденційність і підтримку.

Підготовка до нейродидактичного підходу (для вчителя, вчительки)

- **Чому «м’ясо» на старті? Емоційний гачок.** Мозок підлітка й підлітки краще реагує на емоційно насичену інформацію. Початок з яскравих кейсів активує лімбічну систему (емоції), що підвищує рівень дофаміну, посилює увагу та сприяє кращому запам’ятовуванню. Емоції — це «клей» для знань.

- **Чому симуляція дилем? Активне навчання й проживання досвіду.** Коли учень або учениця «проживає» ситуацію, ухвалюючи рішення, активуються ті самі нейронні мережі, що й у реальному житті. Це формує глибші нейронні зв’язки, ніж пасивне слухання. Це «навчання через дію» (learning by doing), що є надзвичайно ефективним для розвитку критичного мислення та емпатії.

- **Чому групова робота та презентації? Соціальна взаємодія й вербалізація.** Спільне обговорення, аргументація та презентація активують префронтальну кору (планування, аналіз, мовлення), а також соціальні аспекти навчання. Принцип «навчаючи інших, вчишся сам / сама» є одним із найефективніших.

- **Чому мультимодальність (відео, текст, онлайн-дошка)?** Мультимодальність — це використання кількох форматів подання інформації одночасно (наприклад, відео, тексту, звуку чи взаємодії на онлайн-дошці). Коли ми залучаємо різні органи чуття — зір, слух, дотик, — мозок працює активніше, утворюючи міцніші зв’язки. Це допомагає краще запам’ятовувати, розуміти й застосовувати інформацію на практиці. Онлайн-дошка, зокрема, створює відчуття спільної роботи й підвищує залученість.

- **Чому «амигдала/префронтальна кора» та дихальні вправи?** Практична нейронаука. Пояснення базових нейрофізіологічних процесів доступною мовою дає учням та ученицям інструменти для саморегуляції стресу, показуючи, що вміння керувати своїми реакціями — це тренована навичка, а не просто талант. Це дає відчуття контролю та практичної цінності знань.

11 КЛАС. ТРЕНІНГ №7

ІНФОРМАЦІЙНА ВІЙНА

Урок 1 **Тривалість: 45 хв**	**Роль штучного інтелекту в інформаційній війні**

Цілі

За результатами заняття учні та учениці мають:

- усвідомлювати, що таке штучний інтелект (ШІ) і як він застосовується в інформаційній війні;
- знати приклади використання ШІ (генерація контенту, deepfake, автоматизація аналізу даних);
- розпізнавати можливі ризики й негативні наслідки ШІ в інформаційних атаках;
- вміти критично оцінювати інформацію, яка може бути створена або модифікована з допомогою ШІ.

Ключові питання

- Що таке ШІ і які його базові можливості?
- Як ШІ використовується в інформаційній війні (генерація фейків, deepfake, автоматичний аналіз)?
- Які ризики та загрози створення контенту за допомогою ШІ?
- Як захищатися від ШІ-зловживань інформацією?

Реквізит

- Проєктор / екран, презентація.
- Приклади відео або аудіо, які можуть бути deepfake або з елементами модифікації.
- Роздруківки з прикладами (фейків / правди) та критеріями їх оцінки.
- Таймер, маркери, аркуші для груп.

Як підготуватися до заняття:

- Переглянути зібрані матеріали: приклади публікацій із соціальних мереж, де виявлено AI-генерований контент або deepfake.
- Підготувати список критеріїв, що допомагають розпізнати AI-згенерований контент.
- Ознайомитися з джерелами:

Центр протидії дезінформації. Інформаційні операції рф з використанням ШІ у соцмережах
Texty.org.ua. Роль штучного інтелекту у війні

Формат, структура, план заняття

- Міні-лекція
- Робота в групах / парна робота
  Аналіз прикладів
  Дискусія

Час	Етап
1. Вступ (5 хв)	Емоційний гачок. Вчитель / вчителька демонструє перше зображення з презентації і питає учнів та учениць, чи вони зустрічали таке у соцмережах. Учні діляться своїм досвідом. Наступне запитання: «Чи чули ви про відео чи аудіо, яке виявилося не тим, чим здається?» Обговорення. Вчитель / вчителька пояснює, що таке ШІ — алгоритми, які можуть обробляти величезні обсяги даних, генерувати текст, зображення, відео і т. ін.
2. Як ШІ використовується в інформаційній війні (10 хв)	Прогляньте відео за посиланням (10:17-17:42).
3. Аналіз прикладів: deepfake / AI-контент (10 хв)	Об'єднання класу в групи. Кожна група отримує приклад публікації (реальний або змодельований) з соцмереж чи медіа. Завдання: виявити ознаки, що вказують на те, що контент може бути AI-генерованим. Використовують критерії: джерело, якість зображення, голос, анотації, підписи, метадані.
4. Ризики та способи захисту (10 хв)	Обговорення ризиків: вийдіть на теми зниження довіри, маніпуляції настроями, втручання в особисте життя, спотворення фактів. Потім — засоби захисту: медіаграмотність, перевірка джерел, скепсис щодо емоційного контенту, використання фактчекінгових ресурсів.
5. Підсумок і рефлексія (5 хв)	Запитання: «Що з того, що ви дізналися сьогодні, здалося найбільш корисним?» «Як зміняться ваші дії, коли побачите відео чи новину?»
6. Домашнє завдання (5 хв)	Запропонуйте учням та ученицям підготувати алгоритм, як користуватись соцмережами і розпізнавати контент, який згенеровано ШІ. Попросіть їх проговорити це з рідними та друзями.

Урок 2 Тривалість: 45 хв	Кібербезпека в умовах інформаційної війни

Цілі

За результатами заняття учні та учениці мають:

- знати, що таке кібербезпека і чому вона важлива в інформаційній війні;
- знати про загрози від російського месенджера Telegram;
- усвідомлювати основні кіберзагрози: фішинг, шкідливе програмне забезпечення, злом облікових записів, витоки даних тощо;
- знати основи кібергігієни та захисту своєї інформації;
- розуміти роль в освіті, державних ініціативах та співпраці в захисті від кіберзагроз.

Ключові питання

- Що таке кібербезпека і чому вона критична під час війни?
- Які основні кіберзагрози існують зараз?
- Як я можу захистити себе, свої дані, свої пристрої?
- Які державні та громадські ініціативи існують в Україні для підвищення кібербезпеки?

Реквізит

- Презентація.
- Приклади електронних листів-фішингів або підроблених сайтів (скриншоти).
- Роздруківки з правил кібергігієни.
- Аркуші й маркери для вправ.

Формат та план уроку

- Міні-лекція + демонстрація прикладів
- Робота в парах / групах
- Практична вправа «кібергігієна»
- Обговорення ініціатив

Час	Етап
1. Вступ (5 хв)	Запитання: «Хто з вас коли-небудь отримував підозрілий лист?» «А чи приходило вам повідомлення від друга чи подруги з проханням позичити гроші до понеділка?»
2. Основні кіберзагрози (10 хв)	Розкажіть учням та ученицям, які існують небезпеки в цифровому просторі. Для цього скористайтесь презентацією OSINT-агенції Molfar Проговоріть, що таке кібербезпека і для чого вона потрібна? Що таке фішинг? Як краще захистити свої дані? Спробуйте з класом протестувати надійність паролів.
3. Чи несуть загрози месенджери? (10 хв)	Проведіть голосування, якими месенджерами користуються учні та учениці. Обговоріть, які канали найчастіше читають учні та учениці (відповіді фіксуйте на дошці) . Якщо серед переліку начастіше буде згадуватись Труха, прогляньте відео «ЧОМУ не варто читати ТРУХУ» (опційно). Подивіться відео «Telegram – не зовсім надійне джерело новин».
4. Що не можна знімати під час воєнного стану? (5 хв)	Обговоріть, що не можна знімати та публікувати в умовах воєнного стану. Перегляньте відео «Ваші фото розкажуть, де ви! Це легко дізнається ворог»(Spravdi, Dovidka.Info). Проговоріть правила особистої безпеки під час публікацій будь-який фотографій в соцмережах.
5. Практична вправа: кібергігієна (10 хв)	В тих самих групах учні та учениці складають список з 5–7 правил кібербезпеки: наприклад, сильні паролі, двофакторна автентифікація, уважність до посилань, оновлення програм, антивірус, безпечне з'єднання Wi-Fi, відсутність відстежування геолокації. Обговоріть пропозиції учнів та учениць разом; зверніть увагу, які правила повторюються, а які є унікальними для певних груп.
6. Підсумок і рефлексія (5 хв)	Учні та учениці формулюють: «Моя перша дія сьогодні для поліпшення власної кібербезпеки — це...»

Джерела:

1. Dovidka.Info. Загальні рекомендації щодо підвищення рівня безпеки користування смартфонів для цивільних
2. Dovidka.Info. Захист від шпигунського програмного забезпечення
3. Dovidka.Info, Spravdi. Налаштування безпеки у месенджерах
4. Dovidka.Info. Користування VPN для безпеки
5. Dovidka.Info. Кібербезпека під час війни: як захистити інформацію
6. Dovidka.Info. Безпека електронної пошти
7. Dovidka.Info. Безпека ваших пристроїв

Урок 3 Тривалість: 45 хв	Розвідка на основі відкритих джерел (OSINT): цілі та завдання

Цілі

За результатами заняття учні та учениці мають:

- розуміти, що таке OSINT;
- знати, які бувають типи відкритих джерел (наприклад: соціальні мережі, новини, супутникові знімки, бази даних);
- розрізняти типи OSINT-досліджень та вміють застосовувати базові інструменти перевірки.

Ключові питання заняття

- Що таке OSINT і чим він відрізняється від хакінгу чи шпигунства?
- Які є типи OSINT-розслідування?
- Які існують базові інструменти для верифікації локацій?

Як підготуватися до заняття

1. Ознайомитися з презентацією «Про сучасну інформаційну розвідку. Сфери використання».
2. Переглянути зображення з відкритих джерел, відібрані для практичного завдання.
3. Перевірити доступ учнів та учениць до браузера з можливістю зворотного пошуку зображень (Google Images).

Реквізит

- Ноутбуки або смартфони з доступом до інтернету;
- проєктор або інтерактивна дошка.

План заняття

1. Вступ (5 хв)

Запитання до класу:

- «Як можна перевірити, чи справжнє фото, яке ви побачили в соцмережі?»
- «Чи можна дізнатись, де перебувають російські військові, якщо ви маєте лише комп'ютер та інтернет?»

Перегляньте відео та обговоріть, що найбільше вразило у почутому: Molfar. Як малюнки видали інформацію про військове містечко в росії — OSINT (3:36-6:49).

Обговоріть, навіщо нам досліджувати росіян та росіянок, причетних до війни в Україні. Запитайте та зафіксуйте на дошці, що учні та учениці вже знають про OSINT, в яких сферах, окрім фіксації російських злочинів, OSINT може бути корисним.

Додатково: «Телебачення Торонто» має окрему рубрику з розслідуваннями про росіян і росіянок, причетних до російсько-української війни. Можете порекомендувати учням та ученицям переглянути їхні матеріали, щоб більше ознайомитись з тим, які можливості надає OSINT для фіксації військових злочинців та злочинниць.

Телебачення Торонто. російсько-українська війна: OSINT-розслідування

2. Теоретичний блок: «Що таке OSINT і навіщо він потрібен» (10 хв)

1. OSINT (розвідка на основі відкритих даних) — це процес пошуку, аналізу та інтерпретації відкритих даних, які можна отримати легально й етично для певних аналітичних або дослідницьких цілей.

Сьогодні володіння цими навичками стає дедалі важливішим у сферах кібербезпеки, корпоративної розвідки, журналістики та діяльності правоохоронних органів. OSINT допомагає:

- відстежувати потенційні загрози безпеці;
- здійснювати перевірку або розслідування щодо конкретних осіб;
- перевіряти достовірність фактів;
- підтверджувати або спростовувати інформацію з різних джерел;
- виявляти перші сигнали кібератак;
- аналізувати конкурентне середовище;
- оцінювати надійність партнерів чи інших осіб.

Чим це відрізняється від простого пошуку в Google?

Характеристика	**Стандартний пошук / дослідження**	**Розвідка на основі відкритих джерел (OSINT)**
Мета	Загальне розуміння теми, отримання знань.	Підтримка ухвалення конкретного рішення (наприклад, підтвердження особи, викриття зв'язків).
Методологія	Довільна.	Суворо структурована, базується на розвідувальному циклі.
Критичний етап	Збір інформації.	Верифікація та аналіз джерел.
Вихідний продукт	Реферат, стаття, набір фактів.	Аналітичний звіт, висновок.

Джерела OSINT:

1. Традиційні медіа: газети, журнали, телебачення, радіо.
Використовуються для аналізу офіційних повідомлень, політичних заяв, громадських настроїв.

Приклади: BBC, CNN, DW, «Суспільне», «Укрінформ». Можуть містити як первинні свідчення (інтерв'ю, репортажі), так і вторинні інтерпретації (аналітика, коментарі).

2. Інтернет-ресурси.
Офіційні сайти органів влади, міжнародних організацій, партій, компаній.
Новинні сайти та блоги, тематичні форуми.

3. Архіви вебсторінок *(наприклад, Wayback Machine)*.

4. Онлайн-бази даних (державні реєстри, бази компаній, тендери, судові рішення).
Приклади: YouControl, Opendatabot, Реєстр судових рішень.

5. Соціальні мережі.
Платформи типу Facebook, X (Twitter), Instagram, LinkedIn, Telegram, TikTok. Є джерелом інформації про громадські настрої, зв'язки, місцеперебування, діяльність осіб, а також місцем поширення та аналізу первинних свідчень (фото, відео, особисті пости).
Форуми та спеціалізовані спільноти (наприклад, Reddit, тематичні форуми). Містять обговорення, експертні думки, технічні деталі та специфічний сленг, який може бути ключем до розуміння певної спільноти або події.

6. Супутникові знімки.

7. Цифрові метадані.

8. Deep web — контент, який не індексується пошуковими системами.

OSINT — це узагальнене поняття, яке охоплює кілька напрямів збору та аналізу відкритої інформації. Серед них вирізняють такі основні типи:

- **SOCMINT (Social Media Intelligence — розвідка за соціальними мережами) —** аналітика даних із соціальних мереж. Вона базується на вивченні публічної активності користувачів і користувачок, щоб зрозуміти їхні зв’язки, інтереси, настрої чи місцеперебування. Аналіз публікацій, фото, коментарів і взаємодій у Facebook, Instagram, X (Twitter), LinkedIn та інших платформах дозволяє отримати уявлення про громадську думку або поведінку конкретних осіб і груп.

- **HUMINT (Human Intelligence — агентурна розвідка)** — отримання інформації безпосередньо від людей через відкриту комунікацію. До таких методів належать інтерв’ю, спостереження або опитування. Ефективна робота в цій сфері потребує розвинених комунікативних навичок і знання технік соціальної інженерії.

- **GEOINT (Geospatial Intelligence — розвідка геопросторових даних)** — аналіз геопросторових даних, зокрема супутникових знімків, карт і геолокаційної інформації. Цей напрям допомагає відстежувати події у фізичному просторі, оцінювати місцевість та оперативно реагувати на зміни. GEOINT часто використовується у військовій розвідці та кризовому моніторингу.

- **FININT (Financial Intelligence — фінансова розвідка)** — збір і аналіз відкритої фінансової інформації. Цей вид розвідки дає змогу виявляти підозрілі транзакції, корупційні схеми, фінансування терористичних або шахрайських дій, використовуючи дані про інвестиції, активи та фінансові звіти. Важливо пам'ятати про етичний складник цього типу OSINT, бо будь-які адреси чи телефони приватних осіб збирати заборонено.

- **SIGINT (Signals Intelligence — радіоелектронна розвідка)** — дослідження відкритих, доступних сигналів / телеметрії, що легально публікуються. Мета — виявлення комунікаційних ланцюгів, розшифрування повідомлень і визначення намірів або взаємозв'язків учасників / учасниць інформаційного обміну.

Джерело: «Що Таке OSINT у 2025: Гайд від MII».

Ознайомтеся з прикладами різних типів OSINT та кейсами, пов'язаними з дослідженням російсько-української війни.

SOCMINT (Social Media Intelligence)

Яскравим прикладом є розслідування Bellingcat щодо російського спеціального загону швидкого реагування «Ахмат». Після появи влітку 2022 року жахливих кадрів жорстокого сексуального насильства та вбивства українського військового, аналітики й аналітикині Bellingcat розпочали пошук винуватців, маючи лише неякісний відеозапис.

Розслідування, проведене Майклом Шелдоном, розпочалося з пошуку телефонних номерів, які використовувалися для вербування в «Ахмат». Загін активно публікував відео для рекрутингу, що дозволило отримати обличчя низки бойовиків. Наступні кроки включали використання спеціалізованих програм розпізнавання обличчя та пошук їхніх профілів у соціальних мережах. Завдяки цій роботі було знайдено одне фото спецзагону, яке зі свого боку дозволило вийти на його дислокацію поблизу міста Попасна. Цей процес демонструє, як фрагментарні дані із соціальних мереж, поєднані з технічним аналізом, можуть призвести до точної ідентифікації та геолокації.

Волонтери та волонтерки InformNapalm зібрали з відкритих профілів військових фото / пости про переміщення «Буків», чим визначили причетних до збиття росією літака MH17 у 2014 році. Усі зібрані докази були передані до міжнародних судів. У своєму висновку Європейський суд з прав людини зазначив: суд вважає, що автори й авторки звітів, до яких належать Atlantic Council, Bellingcat та InformNapalm, заслуговують на довіру та є серйозними фахівцями й фахівчинями. Отже, немає жодних підстав відкидати свідчення із цих звітів як категорію доказів.

Посилання :

- Медіамейкер. Інколи бойовики самі спрощують роботу. Майкл Шелдон із Bellingcat — про OSINT-пошук російських воєнних злочинців.
- Inform Napalm. Останній рейс російського солдата для MH-17.

GEOINT (Geospatial Intelligence)

Візуалізація розгортання військ РФ, створена Texty.org.ua ще до початку повномасштабного вторгнення, підтверджувала реальну загрозу з боку росії.
Каховська ГЕС (підрив і наслідки). «Схеми» першими опублікували знімки Planet Labs / Maxar; засвідчили руйнування, підтоплення та спроби окупантів відновлювати переправи.

Посилання :

- Texty.org.ua. (Не)прихована загроза: російські військові бази. Супутниковий моніторинг.
- Фейсбук сторінка “Схеми - корупція в деталях”. «Схеми» публікують перший супутниковий знімок зруйнованої Каховської ГЕС.

SIGINT (Signals Intelligence)

У класичному розумінні результати SIGINT не потрапляють у відкритий доступ для загального користування, однак із початком російсько-української війни з’явилися моніторингові канали, що повідомляють про потенційні загрози на основі перехоплених радіоповідомлень.
Одним із прикладів є волонтерський проєкт Monitor: це україномовні OSINT-зведення про активність ворожої авіації та загрозу ракетних обстрілів в Україні.

Посилання :

- WhatsApp канал Monitor - моніторинг ворожої авіації.

HUMINT (Human Intelligence)

Одним із найяскравіших прикладів HUMINT в Україні є спецоперація Головного управління розвідки, під час якої українські розвідники та розвідниці переманили російського пілота бойового гелікоптера Мі-8 на бік України.
Пілот вилетів із території РФ, перетнув лінію фронту та передав гелікоптер українським силам, разом із секретними документами й обладнанням, цінними для розвідки й оборони.

«Список 31» (депортація дітей). «Схеми» + «Ти як?» встановили маршрут вивезення 31 дитини, ідентифікували причетних осіб, використали свідчення батька дітей та документи з верифікованого витоку пошти воєнного злочинця Дениса Пушиліна. Розслідування отримало міжнародні відзнаки й призвело до запровадження санкцій.

Посилання :

- Генеральне управління розвідки України. Операція “Синиця”.
- Радіо Свобода. «Список 31». Як Росія викрадала українських дітей і хто з окупантів до цього причетний.

Доповніть з учнями та ученицями на дошці перелік сфер, в яких може бути використаний OSINT. У переліку мають бути зафіксовані: розвідка даних ворога, журналістські розслідування щодо причетності до шахрайства чи корупції тих чи інших осіб, корпоративні перевірки кандидатів та кандидаток на посаду тощо.

3. Мініпрактикум: «Знайди локацію» (25 хв)

На цьому етапі необхідно навчити учнів та учениць використовувати інструменти зворотного пошуку зображень та поєднувати їх із географічними та лінгвістичними підказками для верифікації та визначення геолокації.

Для цього вам знадобляться:

1. Комп'ютер / ноутбук / планшет із доступом до інтернету (один на пару людей).
2. Інструменти зворотного пошуку: Google Lens, TinEye.
3. Мапи: Google Maps.

Виберіть нейтральне зображення, яке містить:

1. Споруду / пам'ятник, не надто відомий широкому загалу.
2. Текстові підказки (вивіски, дорожні знаки).

3. Унікальні деталі (візерунок бруківки, колір сміттєвого бака, незвичний елемент ландшафту).

4. Бажано, щоб однакове зображення було розміщене на кількох сайтах у різні дати.

Або скористайтесь цими зразками:

Етап 1: зворотний пошук (10 хв)

1. Пошук: виконайте зворотний пошук зображення за допомогою щонайменше двох різних інструментів (наприклад, TinEye та Google Lens).
2. Найдавніше джерело: знайдіть найраніше джерело або оригінальну сторінку (зазвичай Вікісховище, Flickr або особистий блог фотографа / фотографки) та зафіксуйте дату публікації.
3. *Чому це важливо?* Найраніше джерело з найвищою роздільною здатністю найімовірніше є оригіналом, що допомагає у верифікації.
4. Об'єкт: визначте назву об'єкта та його загальне місцезнаходження.

Етап 2: геолокація та верифікація (10 хв)

1. Геопідказки: уважно проаналізуйте зображення. Зверніть увагу на:
   - архітектуру / ландшафт — типові елементи будівель, рослинність;
   - транспорт — номерні знаки, моделі автомобілів, трамваї;
   - вивіски / символіку — прапори, логотипи.
2. Мапа: використовуйте назву об'єкта та знайдені підказки, щоб знайти точне місце на Google Maps або Google Street View.
   - Завдання: зіставте унікальні деталі на фото (вікно, дерево, ліхтарний стовп) з тим, що бачите на Street View.
   - Визначте точну адресу або координати.

Якщо завдання буде виконано швидше ніж заплановано, запропонуйте знайти ще одне зображення того ж місця, але з іншого ракурсу чи в інший час доби (наприклад, у Вікісховищі або на Flickr), щоб підтвердити свою геолокацію. Це навчає кросверифікації.

Таке ж завдання можна виконати з історичними постатями: запропонуйте учням та ученицям фотографії різних маловідомих людей і попросіть знайти про них максимально можливу інформацію, включно з місцем та датою народження.

Етап 3: презентація (5 хв)
Кожна пара коротко представляє:

- Які інструменти використовували?
- Яке найдавніше джерело знайшли та коли воно було опубліковане?
- Точну геолокацію (адресу, місто).
- Які підказки виявилися найкориснішими?

4. Підсумок (5 хв)

Проговоріть з учнями та ученицями 3 речі, які були для них новими, і 3 речі, які вони вже знали.

Підбийте підсумки.

Домашнє завдання

Провести «OSINT-самоаудит» — спробувати знайти інформацію про себе, використовуючи власне ім'я, фото та ніки в соціальних мережах.

Урок 4 Тривалість: 45 хв	Аналіз соцмереж

Цілі

За результатами заняття учні та учениці мають:

- вміти використовувати спеціалізовані сервіси перевірки нікнеймів для пошуку профілів на різних платформах за одним і тим самим ніком;
- вміти застосовувати розширені пошукові оператори Google для цільового пошуку інформації лише у певних соціальних мережах (наприклад, site:facebook.com або site:linkedin.com);
- розуміти, що «цифровий слід» людини часто складається з різних, але пов'язаних між собою публічних профілів, і як ця інформація створює повний портрет.

Ключові питання заняття

- Як один і той самий нікнейм може допомогти знайти людину на десятках різних сайтів?
- Що таке «активний» і «пасивний» цифровий слід?

Реквізит

- Комп'ютери з доступом до інтернету.
- Доступ до кількох соціальних мереж — Facebook, X (Twitter), Instagram — для перевірки результатів.

Як підготуватись до заняття

- Учителю чи учительці слід підготувати кілька безпечних, вигаданих нікнеймів, які потенційно можуть бути зареєстровані на кількох платформах, або використати безпечний приклад, знайдений під час власної підготовки (наприклад, вигаданий нікнейм, який використовується в контексті діяльності публічної організації).

Формат, структура, план заняття		
Етап	**Зміст діяльності**	**Час (хв)**
1. Вступ	Визначення SOCMINT. Пояснення, що таке пасивний збір і чому це наш єдиний фокус. Для демонстрації, як працює SOCMINT, перегляньте та обговоріть відео: Molfar. Пробили анонiма у twitter: Whats my name, TruePeopleSearch + оператори пошуку | OSINT.	**7**
2. Інструмент № 1: перевірка нікнеймів	Пояснення: чому ми використовуємо нікнейми. Демонстрація роботи WhatsMyName на вигаданому нікнеймі. WhatsMyName допоможе знайти профілі людини у соціальних мережах. Для пошуку потрібен лише нікнейм користувача / користувачки, якого / яку ви шукаєте. Цей простий OSINT інструмент дозволяє виявляти присутність особи на різних сайтах та у застосунках. Пошук ведеться через соцмережі, форуми, сайти для обміну фотографіями, відеоплатформи. Інструмент також може допомогти перевірити, чи є знайдені профілі дійсними, порівнюючи дані з різних джерел. **Джерело:** Топ-10 OSINT інструментів 2024 року. Список від аналітиків Molfar.	**10**
3. Інструмент № 2: Google Dorks	Теорія: пояснення операторів site: та " ". Обговорення Google Dorks як методу (нижче описано, що це).	**5**
4. Практичне завдання	Частина А (нікнейм): учні та учениці перевіряють наданий викладачем / викладачкою вигаданий нікнейм. Завдання: знайти 5 платформ, де він зайнятий. Частина Б (Dorks): учні та учениці шукають: 1) фразу «Захист України» лише на site:facebook.com; 2) фразу «БпЛА Вампір» лише на site:facebook.com; 3) фразу «НРК» лише на site:X.com. (нижче описано принцип роботи)	**20**
5. Підсумок	Обговорення: які дані були знайдені (публічні!). Етичні межі: анонімізація і пошана до приватності (нижче описано, що варто пояснити на цьому етапі).	**3**

1. Що таке SOCMINT?

SOCMINT (Social Media Intelligence) — це збір та аналіз інформації, що є у відкритому доступі на платформах соціальних медіа (Facebook, Instagram, X / Twitter, Telegram тощо). Це лише один із доменів OSINT, але ключовий для розуміння публічної думки, зв'язків та переміщень людей.

2. SOCMINT: пасивний vs. активний збір

Для шкільного курсу ми зосереджуємося виключно на пасивному зборі інформації, оскільки він етичний та безпечний.

- **Пасивний збір:** це збір даних без прямої взаємодії з цільовим об'єктом. Аналітик / аналітикиня використовує загальнодоступні пошукові системи, спеціалізовані онлайн-інструменти та реєстри, не залишаючи цифрових «слідів» у системі цілі (тобто не надсилає запити на підтвердження, не здійснює спроб входу). Це наш основний фокус.
- **Активний збір:** це взаємодія з цільовим об'єктом (наприклад, надсилання запиту на додавання в друзі, спроба авторизації для перевірки існування акаунта). Цей метод може залишати сліди та порушувати умови користування платформами, його ми повністю виключаємо.

3. Етичний аспект

Навіть якщо інформація публічна, її використання вимагає етичної відповідальності.

- **Принцип приватності:** не можна використовувати публічно знайдені дані для профілювання або розкриття особистої інформації, якщо це не стосується суспільно важливих розслідувань. **Завжди** працюйте з вигаданими або публічно доступними кейсами, що не зачіпають приватних осіб.

- **Умови платформ:** збір даних має відповідати правилам конкретних платформ (умови використання), порушення може мати юридичні наслідки.

Google Dorks (або Google Hacking) — це не окремий інструмент, а метод використання спеціальних операторів (команд), які дозволяють користувачеві / користувачці фільтрувати мільярди проіндексованих Google сторінок для пошуку дуже специфічної та цільової інформації, недоступної через звичайний пошук.

Це як замість того, щоб просто запитати «де моя книга?», сказати: «Знайди мені книгу (тип об'єкта) про OCINT (ключове слово), яка лежить на сайті шкільної бібліотеки (вказати конкретний сайт)». Цей метод підходить для початківців і початківиць, його активно використовують журналісти, журналістки та слідчі.

Ключові оператори для SOCMINT

Для роботи з SOCMINT та виявлення інформації на конкретних соціальних платформах чи форумах, нам потрібні **два основні оператори**.

Оператор	**Призначення**	**Пояснення для учнів та учениць**	**Приклад використання (SOCMINT)**
site:	Обмеження пошуку доменом	Дозволяє Google шукати інформацію лише на вказаному вебсайті чи соціальній мережі, ігноруючи решту інтернету.	Щоб знайти публічні профілі людини на Facebook: site:facebook.com «Іван Петренко» Київ
" "	Точна відповідність (Exact Match)	Дозволяє шукати точну фразу чи ім'я, а не окремі слова. Виключає небажані варіації.	Щоб знайти публікації з точною фразою: site:facebook.com «Я люблю OSINT»

Додаткові корисні оператори:

Оператор	**Призначення**	**Приклад використання**
-	Виключення слова / фрази	Дозволяє виключити зі списку результатів нерелевантне слово. Наприклад: технічні характеристики БТР -США site:mil.in.ua
****OR або `**	Перегляд альтернативи	Пошук альтернатив Наприклад: новини танки OR БМП site:armyinform.com.ua

Домашнє завдання

Аналіз репутації різних організацій (SOCMINT + Dorks)

Використовуючи розширений пошук, зберіть інформацію та перевірте репутацію у публічному просторі одного з благодійних фондів / спортивної школи / водоканалу / громадської організації, які працюють у вашому регіоні.

Використовуйте оператор site: та оператор " " (точна фраза), щоб знайти згадки про цю громадську організацію чи фонд на неофіційних платформах.

Використовуйте Google Dorks, щоб знайти фотографії чи відеозвіти про роботу цієї організації чи фонду.

Урок 5 **Тривалість: 45 хв**	**GEOINT: що нам кажуть знімки та тіні?**

Цілі

За результатами заняття учні та учениці мають:

- вміти використовувати Google Earth для візуальної верифікації місця, порівнюючи фотографію з картографічними даними, включно з історичними знімками;
- розуміти принцип роботи SunCalc (калькулятора сонячного кута) та вміти застосовувати його для базового аналізу тіней, щоб підтвердити або спростувати час фільмування;
- розуміти, що GEOINT поєднує дані про місцевість, інфраструктуру та природні явища (сонце, тіні) для створення цілісної картини події.

Як підготуватись до заняття

- Кейс для геолокації: підготувати зображення, зроблене у знайомому вчителю / вчительці місці (наприклад, біля школи чи відомого пам'ятника), де є унікальні маркери, але які складно знайти через загальний пошук. Це дозволить учням та ученицям провести практичну геолокацію.

- Кейс для SunCalc: підготувати фотографію, де чітко видно тінь від вертикального об'єкта, зроблену у відомому місці (щоб учні та учениці могли поставити позначку на SunCalc) (як Ейфелева вежа, але в межах вашої громади).

- Перевірка: заздалегідь перевірити, як SunCalc відображає тінь у день та годину проведення уроку, щоб мати наочний приклад.

План заняття	
Етап	**Зміст діяльності**
1. Вступ	Визначення GEOINT та його ролі. Для підкріплення розповіді прогляньте відео, як проводять GEOINT: Molfar OSINT. Кіт пропагандиста виказав його адресу. Алгоритм як робити GEOINT за скрином з відео.
2. Інструмент № 1: Google Earth Pro (візуальна верифікація)	Демонстрація: переходимо від назви міста до конкретних, унікальних деталей про нього. Потім показуємо, як працює функція «історичні знімки» — за її допомогою можна перевірити, як змінювалися територія та ландшафт чи з'являлися нові будівлі. Радимо зробити це на прикладі реального об'єкта у вашому населеному пункті.
3. Інструмент № 2: SunCalc (темпоральний аналіз)	Пояснення: як Сонце та тіні працюють у розслідуванні. Демонстрація: учитель / учителька ставить позначку на карті SunCalc та показує, як змінюється напрямок тіні при зміні часу доби.
4. Практичне завдання	Учні та учениці отримують кейси для геолокації. Завдання: 1) Визначити унікальні об'єкти на фото; 2) Знайти місцевість у Google Earth (або мапах); 3) Перевірити на SunCalc: визначити, чи може тінь на фото відповідати ранку чи вечору на цю дату у цьому місці.
5. Підсумок	Обговорення, що найбільше запам'яталося на уроці. Перегляньте відео, повторіть правила безпеки щодо публікацій цифрового контенту в соціальних мережах. SPRAVDI. «Ваші фото розкажуть, де ви».

Що таке GEOINT?

GEOINT (Geospatial Intelligence) — це аналіз інформації про об'єкти на Землі, отриманої з супутникових знімків, мап, 3D-моделей та геолокаційних даних. У OSINT GEOINT використовується для підтвердження місця та часу фото чи відео.

Ключові методи GEOINT в OSINT

Метод	Суть	Основне завдання
Геолокація	Порівняння візуальних підказок на фотографії (будівлі, знаки, рослинність, рельєф) з картографічними даними (Google Maps, Google Earth).	Знайти точні GPS-координати місця знімання.
Темпоральний аналіз	Використання даних про положення Сонця (тіні) або історичних супутникових знімків.	Визначити дату та час фільмування (чи відповідає заявленим).

Інструмент № 1: Google Earth (картографічна верифікація)

Google Earth — це безплатна програма, яка надає потужні можливості для GEOINT, які виходять за межі звичайних Google Карт.

- 3D-моделювання: можна переглядати місцевість у тривимірному форматі, що допомагає точно зіставити кут знімання фотографії чи відео.
- Історичні знімки: дозволяє переглядати, як виглядала місцевість раніше (наприклад, 2010 чи 2015 року). Це критично важливо, щоб довести, що фото (наприклад, із пошкодженою будівлею) свіже, адже будівля була цілою на торішніх знімках.

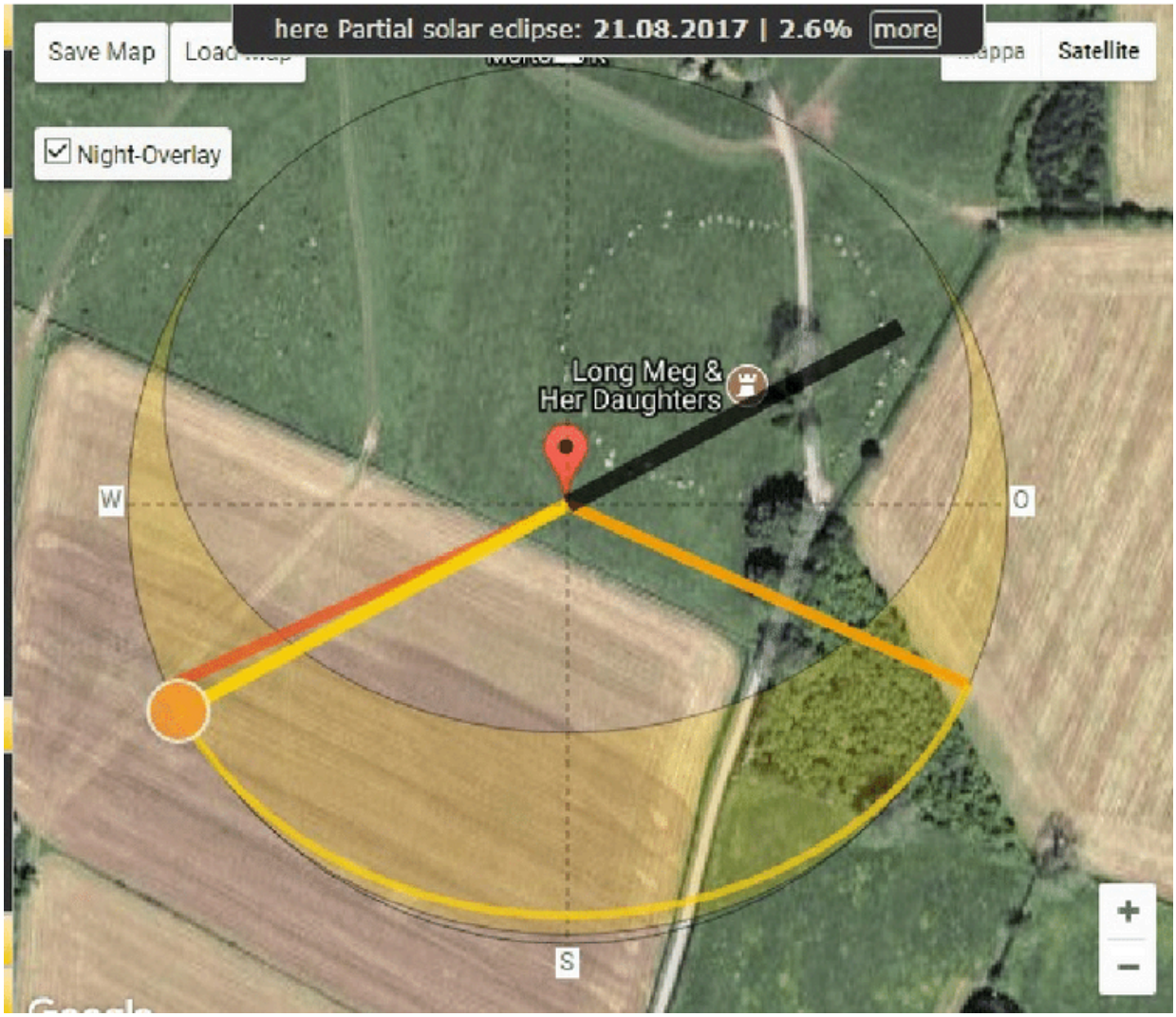
Як активувати перегляд історичних знімків:

Етап демонстрації	Дії вчителя / вчительки в Google Earth	Що це доводить?
1. Актуальний вигляд	Учитель / учителька вводить адресу школи або координати об'єкта і показує його на поточному знімку (3D-модель, якщо доступна).	Геолокація: ми бачимо, що об'єкт існує зараз.
2. Активація «машини часу»	Учитель / учителька активує функцію «історичні знімки» (зазвичай це кнопка, схожа на годинник, на панелі зверху, розділ «Перегляд») і переходить на знімок 2015 року.	Темпоральна верифікація: ми бачимо, що на цьому місці був, умовно, лише пустир, поле чи старий об'єкт.
3. Плавний перехід	**Учитель / учителька пересуває повзунок між 2015 і 2024 роками, показуючи, коли саме почалися зміни (наприклад, 2018 рік).**	**Ми визначаємо точний проміжок часу, коли подія відбулася.**
Висновок	«Якщо хтось опублікує фото цієї будівлі й скаже, що це було знято 15 років тому, ми можемо довести, що це неможливо, адже її тоді не існувало».	

Інструмент № 2: SunCalc (аналіз тіней)

SunCalc — це простий візуальний онлайн-інструмент, який показує траєкторію руху Сонця та напрямок тіней у будь-якій точці земної кулі на будь-яку дату.

- **Принцип:** якщо на фотографії є чітка тінь від об'єкта (наприклад, дерева, стовпа або людини), ми можемо зіставити її напрямок і довжину з тим, що показує SunCalc для цієї геолокації.



Джерело зображення: SunCalc

- **Навчальна цінність:** це показує учням і ученицям, що позиція Сонця залежить від пори року та часу доби. Якщо тінь на фотографії в Києві вказує на південь, а SunCalc показує, що о цій годині тінь мала б вказувати на північ, — це означає, що заявлений час або дата фільмування є неправдивими. Це дуже простий та ефективний спосіб темпоральної верифікації.

Домашнє завдання

Варіант 1: визначити, що знаходиться на місці, де було зроблено фото (дати учням та ученицям безпечне фото будівлі з помітним, але не очевидним орієнтиром — частина пам'ятника, унікальний елемент фасаду, номер будинку).

Варіант 2*: визначити, де саме знаходиться ця колона на відео та підготувати «звіт для командування».

Урок 6 Тривалість: 45 хв	Аналіз фінансових даних

Цілі

За результатами заняття учні та учениці мають:

- вміти користуватися Єдиним державним реєстром юридичних осіб, фізичних осіб — підприємців (ФОП) та громадських формувань (ЄДР) для отримання базових офіційних даних про будь-яку компанію чи приватного підприємця / приватну підприємицю;
- знати, як шукати інформацію у Реєстрі декларацій Національного агентства з питань запобігання корупції (НАЗК) за прізвищем;
- розуміти, що FININT у сфері OSINT стосується виключно публічних даних (реєстрації, майно, судові справи) і є інструментом для перевірки надійності контрагентів та виявлення можливого конфлікту інтересів.

Реквізит

- Комп'ютери з доступом до інтернету.
- Доступ до Єдиного державного реєстру юридичних осіб, фізичних осіб — підприємців та громадських формувань (офіційний портал).
- Доступ до Єдиного державного реєстру декларацій НАЗК.

Як підготуватись до заняття

- **Кейс компанії:** вибрати 1–2 відомі місцеві компанії (або ФОП) для аналізу в ЄДР. Це мають бути реальні, активні компанії з простою історією.

- **Кейс декларації:** вибрати ім'я публічного службовця / публічної службовиці (наприклад, місцевого депутата / місцевої депутатки, міського / міської голови чи урядовця / урядовиці), чиї декларації легко знайти онлайн для демонстрації пошуку на сайті НАЗК.

- **Перевірка:** учителю / учительці слід заздалегідь потренуватися у пошуку в обох реєстрах.

План заняття

Етап	Зміст діяльності	Час (хв)
1. Вступ	Пояснення FININT. Розмежування між публічними реєстрами та соцмережами.	5
2. Інструмент № 1: ЄДР (перевірка компаній)	Демонстрація пошуку за назвою. Пояснення, де знайти: керівника / керівницю, дату реєстрації, дані, чи не перебуває компанія у стані припинення.	10
3. Інструмент № 2: Реєстр декларацій НАЗК	Пояснення ролі НАЗК. Демонстрація пошуку за прізвищем, ім’ям і по батькові публічного службовця / публічної службовиці. Обговорення: які типи майна та доходів вказуються у декларації.	10
4. Практичне завдання	Учні та учениці отримують назву реальної місцевої компанії / ФОП. Завдання: 1) знайти її в ЄДР; 2) визначити точну назву, код ЄДРПОУ та статус (зареєстровано / припинено); 3) знайдену інформацію зафіксувати. Інша група обирає місцевого депутата / місцеву депутатку або голову громади та робить аналіз його / її декларації за останні два роки. Завдання: 1) вибрати ім'я будь-якого місцевого депутата / місцевої депутатки (або голови громади); 2) використовуючи Реєстр декларацій НАЗК, знайти його / її щорічну декларацію за останні два роки; 3) вказати, яку суму річного доходу задекларувала ця особа (фокусуємося лише на цій цифрі, не заглиблюючись у перелік майна).	15
5. Підсумок та анонс	Обговорення. Етика: FININT — лише для справ, що мають суспільний інтерес, або верифікації надійності бізнесу.	5

Що таке FININT в OSINT?

FININT (Financial Intelligence) — це збір та аналіз відкритої, офіційної інформації, що стосується фінансової та майнової діяльності організацій та публічних осіб.

Важливо пояснити учням та ученицям: FININT — це не хакерство, не злам і не доступ до банківських рахунків. Це легальна робота виключно з тими даними, які держава зобов'язана публікувати для забезпечення прозорості та боротьби з корупцією.

FININT дозволяє перевірити:

- Чи існує компанія взагалі (її статус і реєстрацію)?
- Хто її справжній власник / власниця (засновник / засновниця, кінцевий бенефіціар / кінцева бенефіціарка)?
- Чи має компанія борги або судові позови?
- Яким майном володіють публічні службовці / службовиці та їхні родичі й родички (за допомогою декларацій)?

Інструмент № 1: Єдиний Державний Реєстр (ЄДР)

Це найважливіше і найнадійніше джерело для перевірки будь-якої юридичної особи в Україні. Воно вкрай цінне для OSINT, оскільки містить офіційні, перевірені державою дані.

- **Що шукаємо:** наявність реєстрації, точну назву, статус (зареєстровано, у стані припинення, банкрутство), ПІБ керівника / керівниці, основні види діяльності (КВЕД).
- **Чому це важливо:** жодна легальна компанія чи ФОП не може діяти без коректної реєстрації в ЄДР. Перевірка статусу допомагає уникнути співпраці з фірмами-одноденками або такими, що перебувають у процесі ліквідації.

Інструмент № 2: Реєстр Декларацій НАЗК

Це інструмент для забезпечення прозорості та доброчесності влади. Він є публічним і доступним для пошуку за ПІБ декларанта / декларантки.

- **Що шукаємо:** річні доходи, володіння нерухомістю, автомобілями, цінним майном, фінансові зобов'язання, а також інформацію про членів / членкинь сім'ї.
- **Чому це важливо:** це дає змогу виявляти можливі **конфлікти інтересів** або ознаки **незаконного збагачення,** порівнюючи офіційні доходи публічного службовця / службовиці з його / її фактичними активами.

Агрегатори (для контексту)

Існують комерційні платформи (наприклад, YouControl, Opendatabot), які беруть дані з десятків державних реєстрів (ЄДР, судових рішень, реєстр боржників) та об'єднують їх у зручний звіт.

- **Пояснення:** такі платформи спрощують роботу, але для навчання ми зосереджуємося на первинних державних джерелах, щоб учні та учениці розуміли, звідки беруться ці дані.

Домашнє завдання

Варіант 1: знайти фактичний рік заснування відомого українського IT-стартапу (наприклад, Grammarly або Prometheus), а також ім’я одного з його засновників / однієї з його засновниць.

Варіант 2: вибрати велику українську компанію, про яку нещодавно згадували в новинах (наприклад, будівельну фірму або мережу супермаркетів). Знайти її в ЄДР та перевірити, хто є її кінцевим бенефіціарним власником / кінцевою бенефіціарною власницею (або засновником / засновницею). Надати посилання на запис у ЄДР та зазначити ПІБ власника / власниці.

Урок 7 **Тривалість: 45 хв**	**Інструменти OSINT**

Учні та учениці працюють у групах (по 3–4 особи). Їхнє завдання — не виконати розслідування повністю, а розробити детальний, покроковий, етично безпечний план розслідування одного з вигаданих кейсів на 5–6 кроків, вказавши для кожного кроку: що шукаємо, який тип OSINT використовуємо і який інструмент потрібен.

Цей урок — повторення вивченого матеріалу та перевірка, як добре учні та учениці засвоїли визначення типів OSINT та інструментів дослідження.

Приклад заповненого кейсу

Кейс: «Ненадійний забудовник»

Сценарій: у місцевих новинах та соціальних мережах (SOCMINT) активно поширюється інформація про те, що велика будівельна компанія «ЛідерБуд» два тижні тому зупинила роботи на новому житловому комплексі в місті. Клієнти й клієнтки хвилюються, а компанія видалила зі свого сайту всі відгуки.

Завдання: розробити план верифікації надійності компанії та перевірки її репутації.

Після демонстрації прикладу об’єднайте учнів та учениць у групи по 3–4 особи та роздайте їм картки з кейсами.

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	Юридичний статус компанії: чи не перебуває вона у стані припинення або банкрутства?	FININT	ЄДР (Єдиний державний реєстр)
2	Історія репутації: які публічні заяви про терміни будівництва розміщували на сайті компанії до скандалу?	SOCMINT	Google Dorks
3	Перевірка місцевості: чи дійсно роботи зупинені?	GEOINT	Google Earth Pro (огляд свіжих супутникових знімків)
4	Пошук негативу: чи були судові позови, пов'язані з цією компанією?	FININT (Агрегатори)	YouControl / Opendatabot (для демонстрації)
5	Аналіз соцмереж: що люди говорять про компанію зараз на форумах / сторінках, які не пов’язані з компанією?	SOCMINT	Google Dorks (site:facebook.com "ЛідерБуд")

Кейс 1: «Старе фото, видане за нове»

Сценарій: у медіа з’являється фотографія нібито свіжого протесту у місті Х, яку супроводжують заклики до зміни влади. Ви підозрюєте, що фото старе і його використовують для маніпуляції. На світлині чітко видно об'єкт (наприклад, унікальний пам'ятник чи будівлю).

Завдання: розробити план, щоб довести, що фотографія не свіжа або знята не в тому місці.

Кейс 2: «Неофіційні зв'язки місцевого посадовця

Сценарій: про нового місцевого посадовця «Олега Кравченка» (будь-які збіги з реальними людьми — випадкові) стало відомо, що він володіє елітною нерухомістю, яка значно перевищує його офіційні доходи. Також він нібито має тісні зв'язки з власником приватної охоронної фірми «Захист-Т», яка виграє багато державних тендерів.

Завдання: розробити план пошуку офіційних і публічних неофіційних зв'язків посадовця та його активів.

Кейс 3: «Конфлікт інтересів: підрядниця і посадовиця»

Сценарій: міська рада проголосувала за виділення значної суми коштів на ремонт парку. Переможцем тендеру стала Компанія «Містобуд-XXI». У мережі поширюються чутки, що ця компанія належить сестрі або родичці міської посадовиці N (наприклад, членкині бюджетного комітету), яка також раніше була її засновницею.

Завдання: розробити план, щоб підтвердити або спростувати родинні чи ділові зв'язки між посадовицею та компанією.

Кейс 4: «Перевірка постачальника БПЛА»

Сценарій: в Україні створено нову ТОВ «Котики» (вигадана назва), яка оголосила про випуск 1000 БПЛА для потреб армії. Журналістське розслідування виявило, що директор цієї ТОВ раніше володів компанією, яку було ліквідовано за несплату податків. У Facebook-спільнотах поширюються звинувачення, що «Крила перемоги» — шахраї.

Завдання: розробити план перевірки надійності та історії компанії, яка працює у ВПК.

Ключі для вчителя / вчительки:

Кейс 1: «Старе фото, видане за нове»

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	Першоджерело фото: де і коли фото було опубліковане вперше?	SOCMINT / зворотний пошук	Google Images зворотний пошук
2	Геолокація: знайти точне місце знімання за унікальним об'єктом.	GEOINT	Google Earth Pro (перевірка візуальних підказок)
3	Верифікація часу: якщо на фото є тінь, перевірити, чи відповідає її напрямок заявленій порі року або часу доби.	GEOINT	SunCalc
4	Контекст у соцмережах: чи є інші старі згадки про цей протест (з іншими фотографіями), знайдені за допомогою ключових слів?	SOCMINT	Google Dorks (site:X.com "Місто X протест")

Кейс 2: «Неофіційні зв'язки місцевого посадовця»

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	Офіційні активи: перевірити майновий стан і доходи посадовця.	FININT	Реєстр Декларацій НАЗК
2	Компанія «Захист-Т»: хто є керівником та засновником цієї охоронної фірми?	FININT	ЄДР (Єдиний державний реєстр)
3	Перевірка зв'язків у соцмережах: чи публікували посадовець і власник охоронної фірми спільні фото або чи є вони «друзями» в соцмережах?	SOCMINT	Соцмережі
4	Професійні контакти: чи мають вони спільні зв'язки на LinkedIn?	SOCMINT	Google Dorks (site:linkedin.com "Олег Кравченко")
5	Перевірка минулого фірми: чи була «Захист-Т» зареєстрована раніше під іншою назвою, щоб приховати її історію?	Верифікація	Wayback Machine

Кейс 3: «Конфлікт інтересів: підрядниця і посадовиця»

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	**Посадовиця N: які активи та доходи вона задекларувала? Чи згадується у декларації компанія «Містобуд-XXI»?**	**FININT**	**Реєстр декларацій НАЗК (пошук за ПІБ)**
2	Компанія «Містобуд-XXI»: хто є її кінцевим бенефіціарним власником / кінцевою бенефіціарною власницею та засновником / засновницею (ПІБ)?	FININT	ЄДР (Єдиний державний реєстр)
3	Перевірка минулого: чи була посадовиця N засновницею компанії до того, як обійняла посаду?	FININT	ЄДР (за пошуком засновників, засновниць / історії)
4	Неофіційні зв'язки: чи є у публічному доступі фото або спільні згадки посадовиці й власниці компанії?	SOCMINT	Аналіз соцмереж

Кейс 4: «Перевірка постачальника БПЛА»

Крок	Що шукаємо?	Тип OSINT	Інструмент
1	Юридичний статус та історія компанії: хто є поточним керівником та засновником ТОВ «Крила перемоги»? Який її поточний статус?	FININT	ЄДР (Єдиний державний реєстр)
2	Репутація та зміни: як давно існує офіційний сайт компанії та чи змінювалася інформація про її діяльність або керівництво?	Верифікація	Wayback Machine
3	Попередня діяльність: чи згадується ім'я директора компанії у судових реєстрах (або агрегаторах) у зв’язку з несплатою податків чи банкрутством.	FININT	Агрегатори (YouControl / Opendatabot) або Реєстр боржників
4	Інфополе: знайти в інтернеті публікації чи статті, які спростовують або підтверджують звинувачення у шахрайстві, виключивши соцмережі з пошуку.	SOCMINT / Google Dorks	Google Dorks ("Крила перемоги" -site:facebook.com)

Домашнє завдання

Знайти власні цифрові сліди.

Крок	Що шукаємо?	Інструмент	Результат
1	Унікальність нікнейму: на скількох платформах мій основний нікнейм (@ваш_нік) є зайнятим?	WhatsMyName	Кількість зайнятих платформ (наприклад, 7 з 10)
2	Публічні згадки: чи є у Google моє ім'я, прізвище та місто (наприклад, у контексті спортивних змагань, шкільних олімпіад, гуртків)?	Google Search (з оператором " ")	Тип згадок (наприклад, грамоти, результати олімпіад):
3	Специфічні платформи: чи є у Facebook або Instagram мій старий, забутий профіль?	Google Dorks (site:facebook.com "Моє ім'я")	Кількість знайдених публічних акаунтів

Урок 8 **Тривалість: 45 хв**	**Військові професії. Особливості професій, пов'язаних із сучасними цифровими технологіями, медіа та аналізом даних**

Цілі

За результатами заняття учні та учениці мають:

- знати визначення та ключові особливості сучасних військових професій, пов'язаних із цифровими технологіями, медіа та аналізом даних;
- розуміти важливість технологічної підготовки та інтелектуальної праці у сфері національної безпеки та оборони;
- оцінювати перспективи вибору військово-технічної професії та необхідні для цього навички;
- називати приклади реальних військових фахівців і фахівчинь, які ефективно застосовують цифрові технології для захисту країни.

Ключові питання

- Як технологічний прогрес змінив класичні військові професії?
- Які нові військово-технічні спеціальності є найбільш потрібними сьогодні?
- У чому полягає робота військових аналітиків / аналітикинь даних та фахівців / фахівчинь зі стратегічних комунікацій?
- Яка роль відкритих джерел інформації (OSINT) у сучасній розвідці та війні?

Реквізит

- Проєктор та екран / інтерактивна дошка;
- ноутбук з доступом до інтернету.

План заняття

Етап	Час	Діяльність
I. Вступ	5 хв	Вправа «Асоціації»: запитайте учнів та учениць, які 3 слова спадають на думку при згадці словосполучення «військова професія». Презентація теми та цілей.
II. Мінілекція: війна сучасності	10 хв	Пояснення: еволюція військової справи. Детальний огляд на Lobby X професій, які пов'язані з цифровими технологіями, OSINT та медіа. Обговоріть з учнями та ученицями, навіщо війську потрібні такі посади.

III. Ознайомлення з кейсами (20 хв)

Зупиніться на Lobby X на 3 вакансіях: дешифрувальник / дешифрувальниця, аналітик / аналітикиня, пресофіцер / пресофіцерка. На цьому етапі обговоріть з учнями та ученицями, що роблять люди, які проходять службу на знайдених вами вакантних посадах у Силах оборони. Які професійні якості потрібні для того, щоб працювати у цих сферах. Перегляньте відео для кращого розуміння окремих військових спеціальностей.
СБС: Сили безпілотних систем. Хто такий дешифрувальник? Подкаст про професії у війську (01:28–05:50).

Обговоріть, що найбільше вразило, і чи використовує дешифрувальник якісь інструменти, подібні до тих, які ви вже вивчали.

Перейдіть до того, що це не єдина професія у війську, пов'язана з аналізом даних. Запитайте в учнів та учениць, що вони знають про аналітиків та аналітикинь у цивільних сферах — які ролі вони на себе беруть. Запропонуйте ознайомитися з тим, що роблять аналітики та аналітикині у війську.

Перегляньте інтерв'ю з аналітиком Сил безпілотних систем:
СБС: Сили безпілотних систем. Хто такий аналітик в армії? Подкаст про професії у війську (13:37–19:17).

Запитайте в учнів та учениць, як вони можуть описати роботу аналітика чи аналітикині у війську.
Також у Силах оборони не обійтися без людей, які допомагають інформації про військових і підрозділи, в яких вони несуть службу, бути достовірною та потрапляти в медіа.

Хто такі пресофіцери та пресофіцерки?

Уявіть, що військова частина — це великий механізм.
Пресофіцер / пресофіцерка — це його «голос» і «обличчя», людина, яка спілкується зі світом і розповідає про роботу військових. Його / її головне завдання — інформаційна робота. Якщо пояснити просто, він / вона відповідає за те, щоб правдива та важлива інформація про підрозділ (бригаду, батальйон) потрапляла до людей через медіа (інтернет, телебачення, радіо, газети) та соціальні мережі.
Основні обов'язки пресофіцера / пресофіцерки: це багатогранна робота, яка вимагає комунікативних навичок, розуміння медіа та вміння працювати у складних умовах.

- **Комунікація з журналістами / журналістками:**
  - Є головною контактною особою для всіх медіа.
  - Організовує престури та супроводжує журналістів / журналісток (як українських, так і іноземних) на позиції, щоб медіа могли зняти сюжети або написати статті.
  - Стежить за безпекою журналістів і журналісток та дотриманням інформаційної безпеки (щоб не розголошували військові таємниці).
- **Створення власного контенту:**
  - Пресофіцер / пресофіцерка — це часто і журналіст / журналістка, і фотограф / фотографка, і відеограф / відеографка в одній особі.
  - Він / вона знімає фото та відео, бере інтерв'ю у бійців та бійчинь, пише пресрелізи та статті про життя й бойову роботу підрозділу.
- **Ведення соціальних мереж:**
  - Адмініструє офіційні сторінки підрозділу (наприклад, у Facebook, YouTube).
  - Публікує власний контент та матеріали медіа, щоб суспільство бачило роботу військових і їхній героїзм.
- **Інформаційний захист:**
  - Моніторить інформаційний простір, щоб знати, що пишуть про його / її підрозділ.
  - Протидіє фейкам і ворожій пропаганді.

Для ознайомлення з реальними прикладами, зверніться до статті.
Медіамейкер. Що робить пресофіцер у ЗСУ?

V. Підсумки та рефлексія	10 хв	Рефлексія «1 факт, 1 запитання»: кожен учень та кожна учениця називає 1 новий факт, який він дізнався / вона дізналася, і 1 запитання, яке залишилося.

Домашнє завдання

Варіант 1: дослідити біографію військового чи військової, які обіймають посади, пов'язані з сучасними цифровими технологіями, медіа та аналізом даних. Підготувати презентацію на 5–7 слайдів про цю особу.

Варіант 2: пройти курс на Дія.Освіта «Школа OSINT» та скласти квіз для однокласників і однокласниць.

Варіант 3: міні-OSINT-розслідування (5–7 кроків).

Дослідити новину: «Удень 20 серпня російська армія завдала удару по прифронтовій Костянтинівці. Окупанти запустили по місту 8 ракет із системи «Смерч». Вдарили по ринку — у результаті атаки є загиблі та поранені».

Перевірити:

1. **Фото / відео:** зворотний пошук зображень (Google Images).
2. **Місце:** Google Maps, георозмітка.
3. **Дата:** архіви погоди / SunCalc.
4. **Джерело:** хто опублікував фото, відео удару? З якою метою?
5. **Інші публікації:** чи підтверджується достовірність події?
6. **Висновок:** правда / фейк / маніпуляція.
7. **Звіт:** 1–2 сторінки.

Мета: застосувати повний цикл OSINT-розслідування.

Проєкт реалізовувала команда:
Інна Совсун, Анна Коваленко, Вікторія Комарин, Вадим Бейлах, Ірина Кириченко.

В партнерстві з Громадською Організацією «Успішні комунікації»:
Ольга Кутишенко, Оксана Родіонова, Аліса Малицька, Ярема Дух.

При підготовці використані матеріали веб-проєкту **Dovidka.info** Центру стратегічних комунікацій.

Подяки:
12-й бригаді спеціального призначення «Азов» Національної гвардії України за рецензію сценаріїв занять про індивідуальні навички поводження зі зброєю

ГО «Азов.Супровід» за матеріали для розробки уроку «Адаптація суспільства до потреб військовослужбовців і військовослужбовиць та ветеранів і ветеранок війни, зокрема осіб з інвалідністю внаслідок війни»

Демократичній школі «Майбутні» та Тимуру Демчуку за розробку гри «Дві Держави»

OSINT-аґенції Molfar за надані матеріали до тем модуля «Інформаційна війна»

Силам Оборони України та всім українцям та українкам, які борються за нашу свободу і дають можливість працювати над розвитком освіти!