ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«АКАДЕМІЯ ІННОВАЦІЙНОГО РОЗВИТКУ ОСВІТИ»

«ЗАТВЕРДЖУЮ»
Директор ТОВ
«Академія інноваційного розвитку освіти»
вересня 2026 р.
_____Олена ГРОМСЬКА

ПРОГРАМА
підвищення кваліфікації педагогічних та науково-педагогічних працівників закладів освіти

МЕДІАГРАМОТНІСТЬ ТА КІБЕРБЕЗПЕКА: БЕЗПЕЧНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР СУЧАСНОГО ЗАКЛАДУ ОСВІТИ

Київ – 2026

Розробники освітньої програми підвищення кваліфікації педагогічних кадрів: ТОВ «Академія інноваційного розвитку освіти» (***Громська Олена Іванівна,*** директор «Академія інноваційного розвитку освіти»; **Людмила Бондаренко,** заступник директора КУ ЦПР «Освітня траєкторія» ДМР, учитель географії, «учитель-методист», сертифікований тренер «Академії інноваційного розвитку освіти».

Напрям підвищення кваліфікації: розвиток цифрової, інформаційно-комунікаційної, професійно-педагогічної та компетентності щодо створення безпечного освітнього середовища.

Розроблено на основі типової програми: Типова програма підвищення кваліфікації педагогічних та науково-педагогічних працівників з розвитку цифрової компетентності (Наказ МОН України від 03.06.2026 № 871)

Термін дії програми: з 14.09.26 до 14.09.2031 року

Рецензенти:

Пушкарьова Тамара, доктор педагогічних наук, професор, дійсний член (академік) НАПН України, автор і науковий керівник педагогічної технології “Росток” й освітньої інновації «Академія інноваційного розвитку освіти», головний науковий співробітник відділу STEM-освіти Інституту педагогіки НАПН України;

Бурдун Олена Вікторівна, вчитель математики та інформатики вищої категорії, вчитель-методист Ліцея інформаційних технологій № 79 м. Києва, сертифікований тренер «Академії інноваційного розвитку освіти»).

. ПОЯСНЮВАЛЬНА ЗАПИСКА

Актуальність програми: Цифровізація освіти суттєво розширює можливості педагогічних працівників, водночас формуючи нові професійні ризики: інформаційні маніпуляції, дезінформацію, фішинг, соціальну інженерію, шахрайство, витоки персональних даних, кібербулінг, небезпечний цифровий контент, порушення авторського права та некритичне використання контенту, створеного штучним інтелектом.

Особливого значення набуває здатність педагога не лише безпечно користуватися цифровими технологіями, а й навчати здобувачів освіти критично оцінювати інформацію, розпізнавати маніпуляції, перевіряти джерела, відповідально поводитися в цифровому просторі та захищати персональні дані.

Отже, підвищення рівня медіаграмотності та кібербезпеки педагогів є необхідною складовою їхнього професійного розвитку та умовою створення безпечного, інформаційно стійкого й відповідального освітнього середовища.

Цільова група: педагогічні працівники закладів загальної середньої освіти, які забезпечуватимуть реалізацію Державного стандарту базової середньої освіти в другому циклі базової середньої освіти (базове предметне навчання, 7-9 класи).

Обсяг (тривалість): 30 годин (1 кредитів ЄКТС)

Особливості реалізації програми. Програма передбачає навчання педагогічних працівників, які здійснюють освітній процес у закладах загальної середньої освіти, із метою формування в них навичок аналізувати іформаційні повідомлення та визначати ознаки маніпулятивного контенту; перевіряти інформацію за допомогою інструментів фактчекінгу; оцінювати надійність цифрових джерел; розпізнавати фішинг і соціальну інженерію; застосовувати засоби захисту персональних даних, пристроїв та облікових записів;

аналізувати цифровий слід; протидіяти кібербулінгу; безпечно використовувати ШІ; розробляти навчальні завдання з медіаграмотності та кібербезпеки; створювати локальні алгоритми реагування на цифрові загрози. Теоретична складова реалізується через лекції з використанням демонстраційних відео, презентацій, демонстрацій прикладів та відеоматеріалів; практична — через виконання практичних завдань, творчих вправ і проєкту по створенню креативних освітніх матеріалів.

Навчальні заняття проводяться дистанційно з використанням цифрових платформ та інтерактивних інструментів. Опанування курсу відбувається шляхом поєднання теоретичного матеріалу з практичною діяльністю, що забезпечує можливість педагогам одразу застосовувати отримані знання у власній професійній діяльності. Особлива увага приділяється формуванню навичок створення ефективних запитів (промтів), аналізу результатів роботи генеративного штучного інтелекту та усвідомленому використанню можливостей штучного інтелекту в освітньому процесі.

Самостійна робота передбачає опрацювання навчальних матеріалів, виконання практичних завдань, створення власних креативних освітніх продуктів та підготовку до підсумкового оцінювання.

Варіативність тривалості програми: може бути інтенсивна (короткостроковий курс, наприклад, 1-2 тижні, з інтенсивним графіком навчання) або пролонгова форма (тривалий період, проте не більше 4 тижнів).

Форма (форми) підвищення кваліфікації: інституційна (дистанційна).

Мета програми: розвиток професійної цифрової компетентності педагогічних працівників у сфері медіаграмотності, критичного сприйняття інформації, цифрової та кібербезпеки, формування здатності створювати безпечне інформаційно-освітнє середовище та навчати здобувачів освіти відповідальної поведінки в цифровому просторі.

Основні завдання: програма спрямована на поглиблення знань щодо функціонування сучасного медіапростору; розвиток критичного мислення; опанування алгоритмів фактчекінгу; формування вмінь розпізнавати маніпуляції, дезінформацію, фейки та ШІ-контент; розвиток навичок захисту акаунтів, пристроїв і персональних даних; формування алгоритмів реагування на кіберзагрози та розвиток методичної готовності педагогів інтегрувати медіаграмотність і кібербезпеку в освітній процес.

Перелік компетентностей, що вдосконалюватимуться:

Удосконалення раніше набутих та/або набуття нових компетентностей відповідно до професійного стандарту «Вчитель закладу загальної середньої освіти», затвердженого наказом МОН від 29 серпня 2024 року № 1225).

А3. Інформаційно-цифрова компетентність — здатність безпечно, критично, відповідально та ефективно використовувати цифрові технології, цифрові інструменти й ресурси у професійній та освітній діяльності.

Д3. Інформаційно-цифрова компетентність — здатність використовувати цифрові технології в управлінській діяльності, забезпечувати відповідальне й безпечне функціонування цифрового освітнього середовища.

Б2. Інформаційно-комунікаційна компетентність — здатність знаходити, аналізувати, перевіряти, критично оцінювати, систематизувати та використовувати інформацію, здійснювати професійну комунікацію в цифровому середовищі.

Б2.У15. Здатність застосовувати цифрові технології та програмне забезпечення в освітньому процесі — зокрема для роботи з інформаційними та медійними матеріалами, формування медіаграмотності й безпечної цифрової поведінки здобувачів освіти.

ЗК.03. Цифрова компетентність — здатність відповідально використовувати цифрові технології, усвідомлювати цифрові ризики, дотримуватися вимог інформаційної та кібербезпеки.

А1. Здатність планувати і проводити навчальні заняття

А1.У1. Обирати та застосовувати методи, технології та засоби навчання — здатність інтегрувати медіаграмотність, критичне мислення, фактчекінг, цифрову гігієну та основи кібербезпеки у зміст освітнього процесу.

А2.У2. Обирати методи, технології та засоби консультування — здатність здійснювати педагогічний супровід здобувачів освіти щодо відповідального використання цифрових технологій, протидії дезінформації, кібербулінгу, шахрайству та іншим онлайн-загрозам.

В2. Здатність розробляти та вдосконалювати навчально-методичні матеріали

В2.У2. Створювати навчально-методичні матеріали — здатність створювати вправи, кейси, пам'ятки, алгоритми, чек-листи та інші освітні матеріали з медіаграмотності й кібербезпеки.

Очікувані результати підвищення кваліфікації:

Знання й розуміння:

лухач пояснює основні принципи функціонування медіасередовища;

озрізняє факт, судження, рекламу, пропаганду, маніпуляцію та дезінформацію;

арактеризує основні кіберзагрози;

ояснює принципи захисту персональних даних;

озуміє механізми соціальної інженерії, фішингу та кібербулінгу;

ояснює ризики генеративного ШІ та синтетичного контенту.

Уміння:

лухач аналізує медіаповідомлення;

цінює надійність джерел;

еревіряє інформацію, фото та цифровий контент;

дентифікує ознаки фішингових повідомлень;

астосовує багатофакторну автентифікацію та правила кібергігієни;

творює безпечні налаштування цифрового середовища;

озробляє навчальні вправи з медіаграмотності;

оделює алгоритм реагування на кіберінцидент;

цінює ризики використання ШІ-контенту.

Ціннісне ставлення:

лухач демонструє критичне ставлення до інформації;

отримується принципів цифрової етики;

свідомлює відповідальність за поширення інформації;

оважає авторське право та приватність;

отримується принципу «перевір перед тим, як поширювати»;

ідтримує культуру безпечної та ненасильницької цифрової комунікації.

Система та критерії оцінювання результатів підвищення кваліфікації:

Оцінювання відбувається у формі поточного та підсумкового контролів. Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості педагога до виконання конкретних завдань. Під час практичних занять слухачі виконують практичні завдання, у ході яких розробляють цифрові навчальні матеріали, інструменти або освітній контент, що можуть бути безпосередньо використані в їхній педагогічній діяльності. Оцінювання практичних занять має формувальний характер і передбачає надання викладачами рекомендацій щодо покращення результатів роботи, а також залучення слухачів до взаємооцінювання з метою обміну досвідом і підвищення якості створених матеріалів. Форми поточного контролю (оцінювання) – практичні завдання та тестування.

Підсумковий контроль по завершенню курсу здійснюється у формі компетентнісного тестування, яке спрямоване на перевірку рівня сформованості ключових знань, умінь і навичок, визначених програмою. Успішне проходження підсумкового тесту підтверджує досягнення очікуваних результатів навчання та є підставою для зарахування результатів підвищення кваліфікації.

Документ про підсумки підвищення кваліфікації: сертифікат про підвищення кваліфікації, який буде видано слухачам за результатами виконання програми відповідно до вимог постанови КМУ № 800.

Вартість: 1000 грн.

. НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

Програмою передбачено поєднання теоретичного та практичного навчання з використанням дистанційних освітніх технологій і сучасних технологій медіаграмотності.

Особливістю (вид діяльності) є практико-орієнтований підхід.

Самостійна робота передбачає опрацювання навчальних матеріалів, виконання практичних завдань, створення власних освітніх прикладів і підготовку до підсумкового тестування.

Підсумкові заходи включають проходження підсумкового тестування та виконання підсумкового практичного завдання з метою оцінювання рівня засвоєння слухачами змісту Програми, сформованості практичних умінь щодо використання цифрових технологій та інструментів штучного інтелекту в освітньому процесі.

Зміст програми складається з 4 модулів та 11 взаємопов’язаних тематичних блоків.

Розподіл балів за видами активності

Після підрахунку загальної суми балів результат переводиться у підсумкову оцінку, яка вноситься до свідоцтва або журналу оцінок на платформі Moodle:

Сума балів	Оцінка / Рівень	Результат у свідоцтві
90 – 100	Високий (Відмінно)	Зараховано
75 – 89	Достатній (Добре)	Зараховано
60 – 74	Середній (Задовільно)	Зараховано
Менше 60	Незадовільно	Не зараховано

Підсумковий контроль — 20 балів.

Підсумковий контроль здійснюється у формі тестування (12 балів) та виконання підсумкового практичного завдання (8 балів).

Підсумкове тестування спрямоване на перевірку рівня засвоєння теоретичного змісту Програми

Оцінювання здійснюється за результатами виконання практичних і самостійних завдань у межах модулів, а також за результатами підсумкового контролю.

Підсумкове практичне завдання передбачає розроблення та представлення слухачем цифрового освітнього продукту або навчального кейсу, який демонструє здатність використовувати технології медіаграмотності та кібербезпеки у професійній педагогічній діяльності.

Підсумкова практична робота може включати: фрагмент електронного освітнього ресурсу; сценарій або фрагмент уроку з використанням цифрових технологій та ШІ; цифровий інструмент оцінювання або зворотного зв’язку; приклад адаптації навчального матеріалу для різних освітніх потреб учнів; завдання для розвитку цифрової компетентності здобувачів освіти; коротку рефлексію щодо педагогічної доцільності, безпечності та етичності використаних цифрових інструментів.

Учасники, які успішно пройшли навчання, виконали передбачені програмою завдання та набрали не менше прохідного бала, отримують сертифікат про підвищення кваліфікації.

Кількість годин, що відводиться на засвоєння змісту Програми, складає 30 годин, з них: 6 годин — лекційні заняття, 15 годин — практичні заняття, 7 годин — самостійна робота, 2 години — контрольні заходи.

Навчально-тематичний план

Модуль / тема	Лекції	Практичні	Самостійна	Контроль	Усього
Модуль 1. Медіаграмотність педагога	**2**	**4**	**2**	–	**8**
1.1. Сучасний медіапростір та інформаційні виклики	1	1	–	–	2
1.2. Фейки, маніпуляції, пропаганда та дезінформація	1	1	1	–	3
1.3. Фактчекінг та перевірка цифрового контенту	–	2	1	–	3
Модуль 2. Кібербезпека та цифрова гігієна	**2**	**5**	**2**	–	**9**
2.1. Основні кіберзагрози в освітньому середовищі	1	1	–	–	2
2.2. Фішинг, шахрайство та соціальна інженерія	–	2	1	–	3
2.3. Паролі, MFA, пристрої та персональні дані	1	2	1	–	4
Модуль 3. Безпека учасників освітнього процесу	**1**	**4**	**2**	–	**7**
3.1. Цифровий слід і цифрова репутація	–	1	1	–	2
3.2. Кібербулінг та небезпечна онлайн-комунікація	1	2	–	–	3
3.3. Безпечне використання ШІ та синтетичного контенту	–	1	1	–	2
Модуль 4. Медіаграмотність і кібербезпека в освітній практиці	**1**	**2**	**1**	**2**	**6**
4.1. Інтеграція медіаграмотності та кібербезпеки в заняття/урок	1	1	1	–	3

4.2. Практикум «Безпечний цифровий простір закладу освіти»	–	1	–	–	1
Вихідне тестування і захист практичного продукту	–	–	–	2	2
РАЗОМ	**6**	**15**	**7**	**2**	**30**

Це співвідношення свідомо робить програму практикоорієнтованою — 50 % годин відведено практичній роботі, що відповідає логіці Типової програми № 871, де рекомендоване співвідношення становить 30 % лекцій, 50 % практичної та 20 % самостійної роботи.

. ЗМІСТ ПРОГРАМИ

МОДУЛЬ 1. МЕДІАГРАМОТНІСТЬ ПЕДАГОГА

Тема 1.1. Сучасний медіапростір та інформаційні виклики

Інформація та медіа в цифровому суспільстві. Сучасний медіапростір поєднує традиційні медіа, соціальні мережі, цифрові платформи та месенджери. Швидке поширення інформації збільшує ризики фейків, маніпуляцій, пропаганди та дезінформації. Розвиток штучного інтелекту створює нові виклики, зокрема поширення дипфейків і штучно створеного контенту. Тому важливо вміти критично оцінювати інформацію, перевіряти джерела та розрізняти факти й судження. Медіаграмотність і цифрова безпека стають необхідними компетентностями сучасного педагога.

Тема 1.2. Фейки, маніпуляції, пропаганда та дезінформація

Фейки, маніпуляції, пропаганда та дезінформація — це основні інформаційні загрози сучасного медіапростору. Фейки містять неправдиві або вигадані відомості, маніпуляції приховано впливають на сприйняття інформації, а пропаганда формує певні погляди та установки. Дезінформація передбачає навмисне поширення неправдивих чи оманливих повідомлень. Уміння розпізнавати такі впливи, перевіряти джерела й факти є важливою складовою медіаграмотності.

Тема 1.3. Фактчекінг та перевірка цифрового контенту

Практичний фактчекінг: авторство, дата, першоджерело, контекст, підтвердження інформації. Перевірка фото та відеоконтенту.

МОДУЛЬ 2. КІБЕРБЕЗПЕКА ТА ЦИФРОВА ГІГІЄНА

Тема 2.1. Основні кіберзагрози в освітньому середовищі

Основні кіберзагрози в освітньому середовищі — це фішинг, шахрайство, шкідливі програми, злам акаунтів, витік персональних даних і кібербулінг. Особливу небезпеку становлять підозрілі посилання, фальшиві повідомлення та викрадення паролів. Тому педагогам і учням важливо дотримуватися правил цифрової безпеки, захищати особисті дані та відповідально користуватися онлайн-ресурсами.

Тема 2.2. Фішинг, шахрайство та соціальна інженерія

Фішинг, шахрайство та соціальна інженерія — це способи обману користувачів з метою отримання паролів, персональних даних, грошей або доступу до акаунтів. Зловмисники можуть використовувати підроблені листи, повідомлення, сайти, QR-коди та психологічний тиск. Основний захист — критично оцінювати підозрілі повідомлення, перевіряти відправника й посилання та не передавати конфіденційні дані стороннім особам.

Тема 2.3. Паролі, MFA, пристрої та персональні дані

Парольна безпека. MFA. Резервне копіювання. Оновлення програмного забезпечення. Захист персональних даних педагогів, дітей і батьків.

МОДУЛЬ 3. БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ

Тема 3.1. Цифровий слід і цифрова репутація

Цифровий слід і цифрова репутація — це інформація про людину, яка залишається в інтернеті після її онлайн-діяльності: публікації, коментарі, фото,

пошукові запити та реєстрації на сайтах. Вона формує цифрову репутацію та може впливати на особисте й професійне життя. Тому важливо свідомо публікувати інформацію, захищати персональні дані та відповідально поводитися онлайн.

Тема 3.2. Кібербулінг та небезпечна онлайн-комунікація

Кібербулінг та небезпечна онлайн-комунікація — це образи, погрози, переслідування, приниження або поширення приватної інформації через цифрові платформи. Небезпеку також становлять провокації, шантаж, небажані контакти та спроби маніпулювання дітьми в мережі. Важливо вміти розпізнавати такі ситуації, не підтримувати агресивну комунікацію, зберігати докази, блокувати кривдника та звертатися по допомогу.

Тема 3.3. Безпечне використання ШІ та синтетичного контенту

Цифровий слід, репутація, приватність. Кібербулінг, онлайн-насильство, небезпечні контакти. Алгоритм дій педагогічного працівника. Безпечна комунікація з дітьми та батьками. Генеративний ШІ, deepfake, синтетичні фото, аудіо й відео. Перевірка ШІ-контенту. Академічна доброчесність. Типова програма прямо передбачає розвиток здатності розпізнавати кібербулінг, порушення приватності, онлайн-вербування, шахрайство та ризики ШІ-контенту.

МОДУЛЬ 4. МЕДІАГРАМОТНІСТЬ І КІБЕРБЕЗПЕКА В ОСВІТНІЙ ПРАКТИЦІ.

Тема 4.1. Інтеграція медіаграмотності та кібербезпеки в заняття/урок

Методика інтеграції тем у навчальні предмети, заняття ЗДО, виховні години та управлінську діяльність. Створення кейсів, вправ і мінітренінгів. Розроблення пам'ятки, чек-листа або алгоритму реагування на кіберзагрозу.

Тема 4.2. Практикум «Безпечний цифровий простір закладу освіти»

Практикум «Безпечний цифровий простір закладу освіти» спрямований на формування практичних навичок безпечної роботи в цифровому середовищі. Учасники аналізуватимуть типові кіберзагрози, фішингові та шахрайські повідомлення, ситуації кібербулінгу, ризики витоку персональних даних. Практикум передбачає відпрацювання алгоритмів реагування на цифрові загрози та створення правил безпечної онлайн-взаємодії для закладу освіти.

3.1. Орієнтовний перелік практичних завдань

Практична частина курсу спрямована на формування в педагогічних працівників умінь ефективно використовувати технології та інструменти медіаграмотності для організації професійної діяльності.

У межах курсу слухачі виконують такі практичні завдання:

МОДУЛЬ 1. МЕДІАГРАМОТНІСТЬ ПЕДАГОГА

Тема 1.1. Сучасний медіапростір та інформаційні виклики

Мета: сформувати вміння критично аналізувати медіаконтент, визначати інформаційні ризики та перевіряти достовірність повідомлень.

Практичний результат: створення короткого чек-листа «5 кроків перевірки інформації перед поширенням»

Тема 1.2. Фейки, маніпуляції, пропаганда та дезінформація

Мета: навчити розпізнавати недостовірну та маніпулятивну інформацію й застосовувати прості способи її перевірки.

Практичний результат: створення алгоритму «Стоп-фейк: 5 кроків перевірки інформації»

Тема 1.3. Фактчекінг та перевірка цифрового контенту

Мета: сформувати практичні навички перевірки достовірності інформації, фото, відео та онлайн-джерел.

Практичний результат: створення власного алгоритму «Перевіряю перед тим, як довіряти й поширювати».

МОДУЛЬ 2. КІБЕРБЕЗПЕКА ТА ЦИФРОВА ГІГІЄНА

Тема 2.1. Основні кіберзагрози в освітньому середовищі

Мета: навчити педагогів розпізнавати основні кіберзагрози та правильно реагувати на них.

Практичний результат: створення пам'ятки «Кіберзагроза: розпізнай — перевір — захисти — повідом».

Тема 2.2. Фішинг, шахрайство та соціальна інженерія

Мета: сформувати навички розпізнавання шахрайських повідомлень та безпечного реагування на них.

Практичний результат: створення пам'ятки «Не поспішай — перевір — не переходь — не повідомляй дані».

Тема 2.3. Паролі, MFA, пристрої та персональні дані

Мета: сформувати навички захисту облікових записів, пристроїв і персональної інформації.

Практичний результат: створення чек-листа «Мій цифровий захист: пароль — MFA — пристрій — персональні дані».

МОДУЛЬ 3. БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ

Тема 3.1. Цифровий слід і цифрова репутація

Мета: сформувати навички усвідомленого керування власною присутністю та репутацією в цифровому середовищі.

Практичний результат: створення чек-листа «Мій цифровий слід: що про мене бачить Інтернет?».

Тема 3.2. Кібербулінг та небезпечна онлайн-комунікація

Мета: навчити педагогів розпізнавати прояви кібербулінгу та правильно реагувати на небезпечні ситуації в цифровому середовищі.

Практичний результат: створення алгоритму «Кібербулінг: розпізнати — зафіксувати — заблокувати — повідомити — підтримати».

Тема 3.3. Безпечне використання ШІ та синтетичного контенту

Мета: сформувати навички відповідального та безпечного використання ШІ в освітній діяльності.

Практичний результат: створення чек-листа «ШІ безпечно: перевіряй — захищай дані — позначай ШІ-контент — приймай рішення самостійно».

МОДУЛЬ 4. МЕДІАГРАМОТНІСТЬ І КІБЕРБЕЗПЕКА В ОСВІТНІЙ ПРАКТИЦІ.

Тема 4.1. Інтеграція медіаграмотності та кібербезпеки в заняття/урок

Мета: навчити педагогів органічно включати елементи медіаграмотності та кібербезпеки у зміст різних навчальних предметів і занять.

Практичний результат: створення фрагмента уроку/заняття «Предмет + медіаграмотність + кібербезпека», готового для використання в освітньому процесі.

Тема 4.2. Практикум «Безпечний цифровий простір закладу освіти»

Мета: сформувати в педагогів навички комплексного оцінювання цифрових ризиків та організації безпечного цифрового середовища закладу освіти.

Практичний результат: створення «Карти цифрової безпеки закладу освіти» та короткого плану дій «Ризик → профілактика → реагування → відповідальні особи».

. ФОРМИ АТЕСТАЦІЇ ТА ПІДСУМКОВОГО КОНТРОЛЮ

Передбачаються вхідне діагностичне тестування, поточне оцінювання виконання практичних кейсів, вихідне тестування та захист практичного продукту.

Підсумковий практичний продукт слухач обирає відповідно до професійної ролі: сценарій уроку/заняття з медіаграмотності; чек-лист «Кібербезпека педагога»; алгоритм реагування закладу освіти на кіберінцидент; пам'ятка для батьків; мінітренінг для педагогічного колективу; кейс із розпізнавання дезінформації.

Критерії оцінювання: змістова коректність — 25 %; практична застосовність — 25 %; дотримання принципів цифрової безпеки — 20 %; методична доцільність — 20 %; самостійність і аргументованість — 10 %.

Результат вважається успішним за умови виконання не менше 60 % вимог підсумкового оцінювання.

. КОНТРОЛЬ

Вхідне тестування — 15 запитань

Що є основною ознакою надійного інформаційного джерела?

А) емоційний заголовок;

Б) можливість встановити автора і перевірити першоджерело;

В) велика кількість поширень;

Г) яскраве оформлення.

Фактчекінг — це:

А) створення новини;

Б) перевірка достовірності інформації;

В) рекламування;

Г) архівування.

Фішинг — це:

А) спроба отримати конфіденційні дані шляхом обману;

Б) створення відео;

В) пошук інформації;

Г) резервне копіювання.

Найбезпечніший пароль:

А) 12345678;

Б) qwerty;

В) дата народження;

Г) унікальна довга парольна фраза.

MFA означає:

А) багатофакторну автентифікацію;

Б) формат медіафайлу;

В) антивірус;

Г) пошукову систему.

Deepfake — це:

А) синтетично створений або змінений медіаконтент;

Б) архів;

В) пароль;

Г) пошуковик.

Чи можна вважати кількість лайків доказом правдивості?

А) так;

Б) ні.

Що потрібно зробити перед поширенням сенсаційної інформації?

А) перевірити першоджерело та підтвердження;

Б) негайно переслати;

В) змінити заголовок;

Г) додати емодзі.

Соціальна інженерія використовує насамперед:

А) психологічний вплив на людину;

Б) ремонт техніки;

В) програмування;

Г) архівування.

Цифровий слід — це:

А) сукупність даних про активність людини в цифровому середовищі;

Б) вірус;

В) браузер;

Г) пароль.

Найкраща дія після отримання підозрілого посилання:

А) відкрити;

Б) переслати колезі;

В) не переходити та перевірити відправника;

Г) ввести пароль.

Кібербулінг — це:

А) систематичне цькування із застосуванням цифрових засобів;

Б) дистанційне навчання;

В) відеоконференція;

Г) тестування.

Чи потрібно регулярно оновлювати програмне забезпечення?

А) так;

Б) ні.

Чи завжди відповідь генеративного ШІ достовірна?

А) так;

Б) ні.

Хто відповідає за безпечну цифрову поведінку в освітньому середовищі?

А) тільки ІТ-фахівець;

Б) тільки директор;

В) усі учасники освітнього процесу відповідно до своїх ролей;

Г) тільки батьки.

Вихідне тестування — 15 запитань

кий алгоритм найдоцільніший для перевірки сумнівної новини?

А) автор → джерело → дата → контекст → незалежні підтвердження;

Б) лайки → коментарі;

В) дизайн → фото;

Г) кількість репостів.

Лист «Ваш акаунт буде заблоковано через 10 хвилин, введіть пароль» має ознаки:

А) фішингу;

Б) академічного повідомлення;

В) резервного копіювання;

Г) оновлення.

Який засіб найбільше підсилює захист акаунта після пароля?

А) MFA;

Б) один пароль для всіх сервісів;

В) автозаповнення на чужому ПК;

Г) передавання коду колезі.

Що робити з підозрілим вкладенням?

А) не відкривати до перевірки;

Б) одразу завантажити;

В) переслати дітям;

Г) перейменувати.

Найважливіша ознака маніпулятивного повідомлення:

А) спроба вплинути на висновок через емоції або викривлений контекст;

Б) наявність дати;

В) нейтральний стиль;

Г) посилання на першоджерело.

Фото без контексту необхідно:

А) перевірити його походження та контекст;

Б) одразу поширити;

В) обрізати;

Г) додати підпис.

У разі компрометації пароля першою дією є:

А) змінити пароль і перевірити активні сесії/доступи;

Б) видалити браузер;

В) вимкнути монітор;

Г) опублікувати пароль.

Дані дітей у цифровому середовищі потрібно:

А) обробляти відповідально та лише в необхідному обсязі;

Б) публікувати без обмежень;

В) передавати будь-кому;

Г) зберігати у відкритому доступі.

Для перевірки ШІ-контенту педагог має:

А) перевірити факти за надійними джерелами;

Б) автоматично довіряти ШІ;

В) перевірити лише стиль;

Г) орієнтуватися на довжину тексту.

Якщо учень повідомив про кібербулінг, педагог повинен:

А) зафіксувати інформацію та діяти відповідно до встановленого алгоритму реагування;

Б) ігнорувати;

В) публічно обговорити ситуацію;

Г) видалити акаунт учня.

Надійна парольна практика — це:

А) унікальні паролі/парольні фрази та MFA;

Б) один пароль усюди;

В) пароль «123456»;

Г) пароль на стікері біля комп'ютера.

12. Інформаційна бульбашка виникає, коли:

А) користувач переважно бачить контент, що відповідає його попереднім інтересам і поглядам;

Б) комп'ютер перегрівається;

В) зникає інтернет;

Г) пошкоджено файл.

Найкращий спосіб формувати медіаграмотність учнів —

А) систематично включати аналіз реальних інформаційних кейсів в освітній процес;

Б) заборонити інтернет;

В) не обговорювати медіа;

Г) використовувати лише підручник.

Чи можна без перевірки використовувати згенеровану ШІ інформацію в навчальних матеріалах?

А) так;

Б) ні.

Мета кібербезпеки закладу освіти полягає насамперед у:

А) зменшенні цифрових ризиків та захисті людей, даних і освітнього середовища;

Б) забороні технологій;

В) контролі приватного життя педагогів;

Г) скороченні використання цифрових ресурсів.

. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Нормативно-правові документи

а

кон України «Про повну загальну середню освіту» (зі змінами № 4702-

Ь

кон України «Про академічну доброчесність» (№ 4742-IX від

каз Міністерства освіти і науки України від 19 лютого 2021 року № 235

к

а

«Про затвердження типової освітньої програми для учнів 5-9 класів з

аказ Міністерства освіти і науки України від 29 серпня 2024 року № 1225 «Про затвердження Професійного стандарту «Вчитель закладу загальної о

аказ Міністерства освіти і науки України № 1340 від 10.12.2021 «Про затвердження Типової програми підвищення кваліфікації педагогічних працівників з розвитку цифрової компетентності» [Електронний ресурс]. д

іністерство освіти і науки України. Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в о

іністерство освіти і науки України. Інструктивно-методичні рекомендації щодо запровадження та використання технологій штучного інтелекту в м

акон України «Про авторське право і суміжні права» (щодо об’єктів, згенерованих комп’ютерними програмами). URL: і

Основна література

1. Почапська О. І. (Не)безпека в цифровому світі: навчальний посібник. Київ: Академія української преси, Центр вільної преси, 2024. — 59 с. Особливо доречний для тем про цифрові загрози, безпечну комунікацію та поведінку в цифровому середовищі.
2. Мокрогуз О. П., Желіба О. В., Запорожченко М. В. Основи медіаінформаційної грамотності. 10–11 класи: посібник для вчителя / за заг. ред. В. І. Іванова. Київ: Академія української преси, Центр вільної преси, 2024. — 133 с.
3. Інфомедійна грамотність — невід'ємна складова навчального процесу закладу вищої освіти: збірник статей / за заг. ред. В. Ф. Іванова. Київ:

Академія української преси, IREX, Центр вільної преси, 2021. — 400 с. Джерело корисне саме для інтеграції медіаграмотності в освітній процес.

4. IREX. Вправи, які розвивають навички інфомедійної грамотності: навчально-методичне видання. Київ: IREX в Україні, 2020. Практично орієнтоване джерело для роботи з фактами, медіаповідомленнями, маніпуляціями та критичним мисленням.
5. Дія.Освіта. Матеріали з кібергігієни та онлайн-безпеки. Ресурс охоплює захист персональних даних, акаунтів і пристроїв, фішинг, шахрайство, паролі та правила безпечної поведінки онлайн. **Дія.Освіта — Кібергігієна**

Додаткова література

1. Войтович Н. О., Імбіровська-Сиваківська Л. А. Медіаграмотність: технології і практичне застосування / за заг. ред. В. Ф. Іванова. Київ: Академія української преси, Центр вільної преси, 2024. — 57 с. Посібник охоплює критичне мислення, маніпуляції, пропаганду та способи протидії дезінформації. Посібник на порталі «Медіаосвіта і медіаграмотність»
2. Гороховський О. Фактчек. Практичний посібник**.** Видання про методологію фактчекінгу, перевірку публічних заяв, виявлення фейків і маніпуляцій та роботу з інформаційними джерелами. «Фактчек. Практичний посібник»
3. Фактчекінг і медіаграмотність: словник термінів**.** Проєкт «БезБрехні». Практичне довідкове видання для педагогів, тренерів, студентів та учнів, яке допомагає опанувати основні поняття медіаграмотності й фактчекінгу.
   Словник «Фактчекінг і медіаграмотність»
4. Грушевська Ю. А. Медіаграмотність та критичне мислення: навчально-методичний посібник. Одеса: Національний університет «Одеська

юридична академія», 2026. — 70 с. Сучасне українське видання, що охоплює медіаграмотність, фактчекінг, дезінформацію, медіаманіпуляції та інформаційну безпеку. Електронна версія посібника

5. Дія.Освіта. Кібергігієна та онлайн-безпека: освітні матеріали та гайди. Практичні матеріали щодо фішингу, шахрайства, захисту даних, кіберзагроз та безпечної поведінки в цифровому середовищі. Каталог «Кібергігієна та онлайн-безпека»