КОМУНАЛЬНИЙ ЗАКЛАД ЛЬВІВСЬКОЇ ОБЛАСНОЇ РАДИ
«ЛЬВІВСЬКИЙ ОБЛАСНИЙ ІНСТИТУТ ПІСЛЯДИПЛОМНОЇ ПЕДАГОГІЧНОЇ ОСВІТИ»

Кафедра гуманітарної освіти

ПРОГРАМА

підвищення кваліфікації педагогічних та науково-педагогічних працівників

«ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИНІВ: ВІД ТЕОРІЇ ДО ПРАКТИКИ»

Програма підвищення кваліфікації розглянута і рекомендована до затвердження на засіданні кафедри гуманітарної освіти

(протокол №5 від 24 квітня 2026 р.)

Завідувачка кафедри Анна-Марія БОГОСВЯТСЬКА

Програма підвищення кваліфікації затверджена науково-методичною радою

(протокол № 4-2 від 04.06.2026 р.)

Голова науково-методичної ради Павло ХОБЗЕЙ

Розробники: Комунальний заклад Львівської обласної ради «Львівський обласний інститут післядипломної педагогічної освіти» (**Музичук Н.В.**, старша викладачка кафедри гуманітарної освіти КЗ ЛОР «Львівський обласний інституту післядипломної педагогічної освіти»; **Третяк Н.В.**, методистка кафедри гуманітарної освіти КЗ ЛОР «Львівський обласний інституту післядипломної педагогічної освіти», **Козак Т.В.**, методистка кабінету дистанційного навчання КЗ ЛОР «Львівський обласний інституту післядипломної педагогічної освіти»).

Напрям підвищення кваліфікації: розвиток цифрової компетентності педагогічних та науково-педагогічних працівників.

Розроблено: на основі Типової програми підвищення кваліфікації педагогічних та науково-педагогічних працівників з розвитку цифрової компетентності (укладачі: члени робочої групи, склад якої затверджено наказом МОН від 04.03.2026 № 394).

Термін дії програми: з 2026 до 2031 року.

Рецензенти:

Богосвятська А.-М.І., кандидат філологічних наук, доцент, завідувач кафедри гуманітарної освіти КЗ ЛОР ЛОІППО.

Косик В.М., старша викладачка кафедри природничо-математичної освіти і технологій Інституту післядипломної освіти Київського столичного університету імені Бориса Грінченка.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Актуальність програми зумовлена потребою педагогічних працівників закладів освіти впевнено й безпечно використовувати цифрові технології у професійній діяльності. В умовах цифровізації суспільства та освіти, розвитку штучного інтелекту, посилення кіберзагроз і необхідності створення безпечного цифрового освітнього середовища педагоги мають володіти базовими цифровими навичками для організації навчання, комунікації та взаємодії з учасниками освітнього процесу.

Програма спрямована на розвиток цифрової компетентності педагогічних працівників відповідно до сучасних вимог освіти, положень державних стандартів та професійних стандартів педагогічних працівників. Вона враховує європейські й міжнародні підходи до формування цифрової компетентності, зокрема DigCompEdu, UNESCO ICT Competency Framework for Teachers та UNESCO AI Competency Framework for Teachers.

Опанування змісту програми сприятиме підвищенню готовності педагогічних працівників до використання інформаційно-комунікаційних технологій, цифрових освітніх ресурсів та інструментів штучного інтелекту, дотримання правил цифрової безпеки, академічної доброчесності й ефективної роботи в сучасному освітньому середовищі.

Цільова група: педагогічні та науково-педагогічні працівники закладів освіти.

Обсяг (тривалість): 30 годин (1,0 кредитів ЄКТС).

Форма підвищення кваліфікації: інституційна (очна, дистанційна).

Мета підвищення кваліфікації: розвиток цифрової компетентності педагогічних працівників, підготовка їх до професійної діяльності в умовах цифрової трансформації освіти з урахуванням державної політики у сфері освіти, зокрема впровадження цифрових технологій, інструментів штучного інтелекту та європейських орієнтирів розвитку.

Завдання підвищення кваліфікації:

- поглиблення знань слухачів із питань безпеки в цифровому суспільстві та цифровому освітньому середовищі закладу освіти;

- розширення розуміння слухачів щодо особливостей організації освітнього процесу з використанням цифрових технологій;
- розвиток у слухачів уміння відповідально використовувати інструменти штучного інтелекту для підготовки навчальних матеріалів, організації освітнього процесу та підтримки навчання здобувачів освіти;
- мотивація слухачів до проєктування, створення, поширення нових електронних (цифрових) освітніх ресурсів із відповідних предметів/інтегрованих курсів;
- розвиток у слухачів уміння застосовувати цифрові технології для моніторингу, контролю та об'єктивного оцінювання результатів навчальної діяльності здобувачів освіти, аналізу освітніх даних, а також зворотного зв'язку та рефлексії.

Перелік компетентностей, що вдосконалюватимуться/набуватимуться:

А.3. Інформаційно-цифрової, через здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею в професійній діяльності; ефективно використовувати наявні та створювати (за потреби) нові електронні (цифрові) освітні ресурси; використовувати цифрові технології в освітньому процесі (відповідно до рівня освіти, який надається).

Д.1. Інноваційної, через здатність застосовувати наукові методи пізнання в освітньому процесі; використовувати інновації в професійній діяльності; застосовувати інноваційні підходи до розв'язання проблем у педагогічній діяльності.

Очікувані результати підвищення кваліфікації: за результатами навчання слухачі/слухачки зможуть:

• пояснювати основні види кіберзагроз, кіберзлочинів і ризиків цифрового освітнього середовища;

• застосовувати правила кібергігієни, захисту персональних даних, приватності та цифрової ідентичності учасників освітнього процесу;

• розпізнавати прояви фішингу, дезінформації, кібербулінгу, грумінгу та інших онлайн-ризиків, добирати способи реагування й профілактики;

• розробляти практичні матеріали й елементи шкільної політики безпеки для запобігання кіберзлочинам у закладі освіти.

Система та критерії оцінювання результатів підвищення кваліфікації:

Контроль та оцінювання знань слухачів проводиться послідовно й систематично: під час практичних занять, виконання інтерактивних вправ, аналізу кейсів, обговорення результатів групової роботи, вхідного та вихідного діагностування. **Оцінювання вербальне**

Особливості реалізації програми: очна форма навчання, поєднання коротких теоретичних блоків, практичних вправ, групової взаємодії й виконання індивідуальної роботи.

Документ про підвищення кваліфікації: сертифікат видається відповідно до кількості прослуханих годин за умови відвідування не менше 50% занять.

2. НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

Назва навчальних тем	Кількість годин				
	Лекції	Практичні заняття	Самостійна робота	Контрольні заходи	Усього
1	2	3	4	5	6
Попередження кіберзлочинів: від теорії до практики					
Тема 1.1. Інформаційно-комунікаційна компетентність здобувачів освіти. Безпечне навчальне середовище. Кіберзлочинність	1	2	1		4
Тема 1.2. Інформаційна та медіаграмотність здобувачів освіти. Приватність. Особиста безпека в Інтернеті. Навички кібергігієни. Експлуатація дітей в Інтернеті. Дезінформація.	1	3	2		6
Тема 1.3. Безпечне та відповідальне використання цифрових технологій і сервісів здобувачами освіти для співпраці, комунікації та створення контенту. Життєві навички, мережева етика та мережевий етикет. Кібербулінг. Кібернасильство проти жінок та дівчат.	1	3	2		6
Тема 1.4. Технічна самостійність здобувачів освіти та розв'язання проблем у цифровому освітньому	2	3	1		6

середовищі. Цифрове громадянство. Цифровий слід. Грумінг та безпека.					
Тема 1.5. ШІ грамотність здобувачів освіти. Стратегії запобігання кіберзлочинам. Стратегічне планування: розробка шкільної політики безпеки.	2	3	1		6
Підсумкові заходи				2	2
Разом за програмою	**7**	**14**	**7**	**2**	**30**

3. ЗМІСТ ПРОГРАМИ

Попередження кіберзлочинів: від теорії до практики

Тема 1.1. Інформаційно-комунікаційна компетентність здобувачів освіти. Безпечне навчальне середовище. Кіберзлочинність.

Поняття інформаційно-комунікаційної компетентності здобувачів освіти та її значення для безпечної участі в цифровому середовищі. Ознаки безпечного цифрового освітнього простору: захищені акаунти, налаштована приватність, відповідальна онлайн-комунікація, безпечне використання пристроїв і сервісів. Основні види кіберзлочинів, що можуть загрожувати учасникам освітнього процесу: фішинг, шахрайство, крадіжка облікових даних, злам акаунтів, поширення шкідливого програмного забезпечення, виманювання персональної інформації. Роль педагога у формуванні навичок безпечної поведінки учнів та організації профілактичної роботи в закладі освіти.

Практична складова. Аналіз типових ситуацій кіберризиків у шкільному середовищі; визначення правил безпечного користування освітніми платформами, електронною поштою, месенджерами та хмарними сервісами.

Тема 1.2. Інформаційна та медіаграмотність здобувачів освіти. Приватність. Особиста безпека в Інтернеті. Навички кібергігієни. Експлуатація дітей в Інтернеті. Дезінформація.

Формування навичок критичного пошуку, перевірки й оцінювання інформації в цифровому середовищі. Приватність і персональні дані: що можна і чого не варто публікувати онлайн, як налаштовувати безпеку профілю, паролі та двофакторну автентифікацію. Основи кібергігієни для учнів і педагогів: оновлення програм, безпечні посилання, перевірка джерел, обережність із вкладеннями, захист пристроїв. Онлайн-експлуатація дітей, небезпечні

контакти, шантаж, маніпуляції та алгоритм звернення по допомогу. Дезінформація, фейки, маніпулятивні повідомлення, дипфейки та ШІ-згенерований контент як чинники ризику для безпеки дитини.

Практична складова. Розбір кейсів фішингових повідомлень, фейкових новин і небезпечних онлайн-контактів; створення чекліста кібергігієни для класу або педагогічного колективу.

Тема 1.3. Безпечне та відповідальне використання цифрових технологій і сервісів здобувачами освіти для співпраці, комунікації та створення контенту. Життєві навички, мережева етика та мережевий етикет. Кібербулінг. Кібернасильство проти жінок та дівчат.

Відповідальне використання цифрових сервісів для навчання, спільної роботи, комунікації та створення контенту. Правила мережевої етики: повага до співрозмовника, недопущення мови ворожнечі, коректне поширення матеріалів, дотримання авторського права. Кібербулінг: ознаки, форми, наслідки для дитини, алгоритм реагування педагога та закладу освіти. Кібернасильство проти жінок та дівчат: онлайн-переслідування, погрози, поширення приватних матеріалів, гендерно зумовлені образи, механізми підтримки й перенаправлення до фахівців. Формування життєвих навичок безпечної цифрової взаємодії: емпатія, асертивність, відповідальність, уміння звертатися по допомогу.

Практична складова. Розроблення правил безпечної онлайн-комунікації для учнів; моделювання дій педагога у випадку кібербулінгу або поширення образливого контенту.

Тема 1.4. Технічна самостійність здобувачів освіти та розв’язання проблем у цифровому освітньому середовищі. Цифрове громадянство. Цифровий слід. Грумінг та безпека.

Розвиток технічної самостійності здобувачів освіти: уміння виявляти прості технічні проблеми, діяти безпечно під час збоїв, звертатися до надійних джерел допомоги. Цифрове громадянство як відповідальна участь у цифровому суспільстві: права, обов’язки, безпечна поведінка, повага до інших, відповідальність за власні дії онлайн. Цифровий слід і цифрова репутація: довготривалі наслідки публікацій, коментарів, фото, відео та даних, які залишаються в мережі. Грумінг: ознаки небезпечної комунікації з дорослими в інтернеті, способи маніпуляції, правила безпеки та порядок реагування.

Практична складова. Проведення аудиту цифрового сліду на прикладах; складання пам’ятки для учнів щодо безпечного спілкування онлайн і дій у разі підозрілих контактів.

Тема 1.5. ШІ-грамотність здобувачів освіти. Стратегії запобігання кіберзлочинам. Стратегічне планування: розробка шкільної політики безпеки.

ШІ-грамотність як складова цифрової компетентності: базове розуміння можливостей і ризиків штучного інтелекту, критичне оцінювання ШІ-згенерованого контенту, перевірка фактів і джерел. Ризики використання ШІ в контексті кібербезпеки: створення фішингових повідомлень, дипфейків, маніпулятивного контенту, автоматизованого шахрайства, порушення приватності. Стратегії запобігання кіберзлочинам у закладі освіти: профілактика, навчання, реагування, комунікація з батьками, фіксація інцидентів, співпраця з адміністрацією та відповідними службами. Розроблення шкільної політики безпеки: правила користування цифровими сервісами, захист персональних даних, алгоритми повідомлення про інциденти, підтримка постраждалих, регулярне оновлення правил.

Практична складова. Проєктування фрагмента шкільної політики цифрової безпеки або плану профілактичного заняття для учнів із теми кібербезпеки.

Підсумкові заходи. Презентація практичної роботи слухачів/слухачок: чекліста, пам’ятки, кейсу, мініуроку або фрагмента шкільної політики безпеки. Обговорення результатів, самооцінювання, рефлексія щодо можливостей упровадження напрацьованих матеріалів у закладі освіти.

4. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Нормативно-правові документи

1. Верховна Рада України. Закон України «Про освіту» № 2145-VIII. https://zakon.rada.gov.ua/laws/show/2145-19#Text

2. Верховна Рада України. Закон України «Про повну загальну середню освіту» № 463-IX. https://zakon.rada.gov.ua/laws/show/463-20#Text

3. Верховна Рада України. Закон України «Про захист персональних даних» № 2297-VI. https://zakon.rada.gov.ua/laws/show/2297-17#Text

4. Верховна Рада України. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Верховна Рада України. Закон України «Про авторське право і суміжні права» № 2811-IX. https://zakon.rada.gov.ua/laws/show/2811-20#Text

6. Кабінет Міністрів України. Концепція розвитку цифрових компетентностей (№ 167-р). https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

7. Міністерство освіти і науки України. Професійний стандарт «Вчитель закладу загальної середньої освіти» (№ 1225). https://register.nqa.gov.ua/uploads/0/646-ilovepdf_merged.pdf

8. Міністерство освіти і науки України, Міністерство цифрової трансформації України. Інструктивно-методичні рекомендації щодо запровадження та використання технологій штучного інтелекту в закладах загальної середньої освіти. https://ai.thedigital.gov.ua/documents

9. European Commission. DigComp 2.2: The Digital Competence Framework for Citizens. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

10. European Commission. DigCompEdu: European Framework for the Digital Competence of Educators. https://publications.jrc.ec.europa.eu/repository/handle/JRC107466

11. UNESCO. AI competency framework for teachers. Paris: UNESCO, 2024. DOI: 10.54675/ZJTE2084.

Основна література

1. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання: навч.-метод. посіб. / С. О. Доценко, В. В. Ворожбіт-Горбатюк, Т. М. Собченко. Харків: Вид-во «Ранок», 2021. 192 с.

2. Морзе Н., Базелюк О., Воротнікова І., Дементієвська Н., Захар О., Нанаєва Т., Чернікова Л. Опис цифрової компетентності педагогічного працівника. Відкрите освітнє е-середовище сучасного університету, 2019. https://doi.org/10.28925/2414-0325.2019s39

3. Воротникова, І. П. Умови формування цифрової компетентності вчителя у післядипломній освіті. Відкрите освітнє е-середовище сучасного університету, 2019, (6), 101–118. https://doi.org/10.28925/2414-0325.2019.6.9

4. Міністерство цифрової трансформації України. Дослідження цифрової грамотності в Україні. Київ, 2023. https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

5. UNESCO. Guidance for generative AI in education and research. Paris: UNESCO, 2023. https://unesdoc.unesco.org/ark:/48223/pf0000386693

6. Vuorikari, R., Kluzer, S., Punie, Y. DigComp 2.2: The Digital Competence Framework for Citizens – With New Examples of Knowledge, Skills and Attitudes. Luxembourg: Publications Office of the European Union, 2022. DOI: 10.2760/115376

7. Штучний інтелект — асистент сучасного вчителя: навч. посіб. / С. Доценко, В. Ворожбіт-Горбатюк, Т. Собченко, М. Корнієнко. Харків: Вид-во «Ранок», 2025. 176 с.

Електронні ресурси

1. Національна онлайн-платформа цифрової грамотності «Дія.Освіта». https://osvita.diia.gov.ua/

2. Дія.Освіта. Основи кібергігієни. https://osvita.diia.gov.ua/courses/cyber-hygiene

3. Дія.Освіта. Персональна кібергігієна. https://osvita.diia.gov.ua/courses/personal-cyberhygiene

4. Дія.Освіта. Кібергігієна: як захиститися від фішингу. https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu

5. Дія.Освіта. Обережно! Кібершахраї. https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters

6. Дія.Освіта. Кібергігієна для молоді. https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth

7. Дія.Освіта. Персональні дані. https://osvita.diia.gov.ua/courses/personaldata

8. Дія.Освіта. Онлайн-безпека для освітян. https://osvita.diia.gov.ua/simulators/onlajn-bezpeka-dla-osvitan

9. Дія.Освіта. Онлайн-безпека для підлітків. https://osvita.diia.gov.ua/simulators/e-safety-teens-simulator

10. Дія.Освіта. Онлайн-безпека для дітей. https://osvita.diia.gov.ua/simulators/e-safety-children-simulator

11. Дія.Освіта. Безпека дітей в інтернеті для батьків. https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey

12. Дія.Освіта. Школа без цькувань. Учителю. https://osvita.diia.gov.ua/en/courses/skola-bez-ckuvan-castina-1-ucitelu

13. Дія.Освіта. Як захиститися від фейків і дезінформації. https://osvita.diia.gov.ua/courses/how-to-protect-yourself-from-fakes-and-disinformation

14. Дія.Освіта. Школа OSINT. https://osvita.diia.gov.ua/courses/osint-school

15. Всеукраїнська школа онлайн. https://lms.e-school.net.ua/

16. SELFIE for Teachers: інструмент самооцінювання цифрової компетентності педагогічних працівників. https://educators-go-digital.jrc.ec.europa.eu/