

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

ЗАТВЕРДЖУЮ

Проректор з навчально-педагогічної роботи

Ігор ЧОРНОДІД

«31» серпня 2026 року

ПРОГРАМА ПРАКТИКИ

ОК11

Переддипломна практика

Освітньо-професійна програма

«Професійна освіта. Управління інформаційною безпекою»

Другий (магістерський) рівень вищої освіти

Спеціальність А5 Професійна освіта (за спеціалізаціями)

Галузь знань А Освіта

Денна та заочна форми навчання

Мова викладання — українська

Київ 2026

Відомості про розроблення і погодження

Укладачі: Кашина Ганна Сергіївна; Нізовцев Юрій Юрійович; Брезецький Сергій Олександрович.

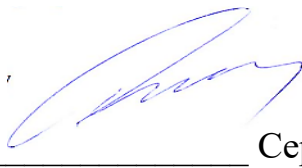
Робочу програму розглянуто на засіданні кафедри інтелектуальних систем та цифрових технологій

Протокол № 1 від «27» серпня 2026 року.

Завідувач кафедри  Ганна КАШИНА

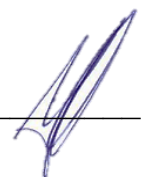
Рекомендовано Вченою радою факультету економіки, соціальних технологій та туризму.

Протокол № 1 від «27» серпня 2026 року.

Декан факультету  Сергій ШОЛУДЧЕНКО

Схвалено науково-методичною радою Академії

Протокол № 1 від «31» серпня 2026 року.

Голова ради  Ігор ЧОРНОДІД

© АПСВіТ, 2026 рік

© Ганна КАШИНА, Юрій НІЗОВЦЕВ, Сергій БРЕЗЕЦЬКИЙ, 2026 рік

1 Опис освітнього компонента

Показник	Зміст
Статус	Обов'язковий освітній компонент
Обсяг	11 кредитів ЄКТС; 330 годин
Семестр	3
Форма контролю	Залік із захистом звіту
Організація навантаження	330 годин розподілено за етапами. Консультації, робота на базі, підготовка матеріалів і звіту входять у цей обсяг та не додаються понад нього.
Підсумковий продукт	Звіт і пакет матеріалів апробації магістерського дослідження з протоколом походження даних.

Відповідальна — Кашина Г. С.; Нізовцев Ю. Ю. та Брезецький С. О. — профільний супровід за темою завдання.

2 Мета завдання та місце компонента

Забезпечити виконання погодженого дослідницького завдання, збирання й аналіз матеріалів, апробацію рішення та формування доказової основи магістерського дослідження.

Завдання конкретизуються через такі професійні дії: погодити дослідницьке завдання, календар і перелік дозволених матеріалів; побудувати опис об'єкта, реєстр релевантних активів і карту проблем; зібрати дозволені дані або сформулювати погоджений модельний набір із журналом походження.

2.1 Передумови та наступність

ОК2, ОК7, ОК8, ОК9 та ОК10. До початку погоджуються тема дослідження, індивідуальне завдання, база, керівництво й умови доступу до даних.

Пакет даних, протоколи й результати апробації передаються до ОК12 із дотриманням конфіденційності та без подвійного обліку витрачених годин.

3 Заплановані компетентності та результати навчання

Коди й формулювання наведено за матрицями чинної робочої редакції ОПШ. Компонент робить внесок у зазначені результати; їх досягнення перевіряється сукупністю передбачених програмою завдань. Інтегральна компетентність реалізується через виконання комплексного професійного завдання.

Код	Компетентність
ІК	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру і проблеми у професійній освіті.
ЗК1	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК3	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
ЗК6	Здатність діяти соціально відповідально та свідомо.
СК1	Здатність застосовувати і розробляти нові підходи до вирішення задач дослідницького та/або інноваційного характеру і проблем професійної освіти.
СК4	Здатність аналізувати, прогнозувати, критично осмислювати проблеми у професійній освіті, приймати ефективні рішення щодо їх розв'язання.
СК5	Здатність розробляти і реалізовувати проекти у професійній освіті, у тому числі міждисциплінарні, здійснювати їх інформаційне, методичне, матеріальне, фінансове та кадрове забезпечення.
СК7	Навички консультування у сфері професійної освіти.
СК9	Здатність забезпечувати академічну доброчесність, цифрову етику та відповідальне використання цифрових технологій і штучного інтелекту в професійній освіті.
СК10	Здатність ідентифікувати інформаційні активи освітньої організації, оцінювати ризики інформаційної безпеки та обґрунтовувати організаційні й технічні заходи їх оброблення.
СК11	Здатність розробляти, впроваджувати й оцінювати політики та процедури управління інформаційною безпекою цифрового освітнього середовища з урахуванням вимог законодавства і захисту персональних даних.

Код	Компетентність
СК12	Здатність аналізувати кіберінциденти в освітньому середовищі, застосовувати цифрову аналітику та інструменти штучного інтелекту з перевіркою достовірності їх результатів і збереженням людського контролю.
СК14	Здатність організовувати командне реагування на інциденти інформаційної безпеки, планувати відновлення освітніх сервісів і забезпечувати безперервність освітнього процесу.

3.1 Результати та докази їх досягнення

Результат навчання за ОПП	Доказ у межах компонента
РН2. Ефективно використовувати сучасні цифрові інструменти, інформаційні технології та ресурси у професійній, інноваційній та/або дослідницькій діяльності.	Перевірений цифровий продукт, аналітична процедура або демонстрація доречного використання інструмента.
РН8. Здійснювати у науковій та професійній літературі, базах даних, інших джерелах пошук необхідної інформації з професійної освіти і дотичних питань, систематизувати, аналізувати та оцінювати відповідну інформацію.	Перевірений огляд джерел, стратегія пошуку та критичне зіставлення відомостей.
РН9. Будувати і досліджувати моделі процесів у галузі професійної освіти.	Модель освітнього процесу або досліджуваної ситуації з явними припущеннями та способом перевірки.
РН10. Здійснювати консультативну діяльність у сфері професійної освіти.	Консультаційна записка, рольова консультація або погоджені рекомендації учасникам освіти.
РН12. Дотримуватися принципів академічної доброчесності та цифрової етики, відповідально використовувати цифрові технології й штучний інтелект, забезпечувати прозорість, безпеку та етичне управління освітніми даними.	План роботи з даними, перевірені посилання та декларація використання цифрових і AI-інструментів.

Результат навчання за ОПП	Доказ у межах компонента
РН13. Ідентифікувати та класифікувати інформаційні активи цифрового освітнього середовища, будувати модель загроз, оцінювати ризики й обґрунтовувати план їх оброблення з визначенням відповідальних осіб, ресурсів і показників результативності.	Опис активів, модель загроз, критерії оцінки ризиків або відповідний дослідницький фрагмент.
РН14. Розробляти політики та процедури інформаційної безпеки освітньої організації, визначати правила доступу, оброблення і захисту персональних даних, резервного копіювання та контролю виконання встановлених вимог.	Проект чи аналіз політики доступу, приватності, резервування та відповідальності.
РН15. Аналізувати дані про кіберінциденти, документувати висновки, визначати пріоритети реагування та план відновлення цифрових освітніх сервісів, оцінювати обмеження й похибки інструментів штучного інтелекту.	Аналітичний звіт про інцидент, перевірка висновків і сценарій реагування або відновлення.
РН16. Проектувати та реалізовувати цифровий освітній проєкт із визначеними вимогами до інформаційної безпеки, керувати командною взаємодією, ресурсами і ризиками та оцінювати педагогічну й організаційну результативність проєкту.	План освітнього проєкту, ресурсне обґрунтування та спосіб оцінювання педагогічного ефекту.

4 Зміст програми

Етап 1 Узгодження дослідницького завдання

Уточнення проблеми, мети й плану магістерського дослідження. Вивчення можливостей бази практики та умов доступу до даних. Узгодження етичних і організаційних обмежень.

Очікувана дія: Погодити дослідницьке завдання, календар і перелік дозволених матеріалів.

Етап 2 Дослідження об'єкта і ризиків

Опис освітнього процесу, цифрового середовища й інформаційних активів у межах теми. Виявлення проблем, загроз та вимог користувачів. Перевірка джерел і припущень.

Очікувана дія: Побудувати опис об'єкта, реєстр релевантних активів і карту проблем.

Етап 3 Збирання та підготовка матеріалів

Реалізація погодженої процедури збирання даних. Контроль якості, знеособлення, робочі копії та документування перетворень. Чітке позначення синтетичних або модельних матеріалів.

Очікувана дія: Зібрати дозволені дані або сформувати погоджений модельний набір із журналом походження.

Етап 4 Апробація запропонованого рішення

Розроблення й випробування педагогічного, управлінського або інформаційно-безпекового рішення. Критерії оцінювання, фіксація виконаних дій і порівняння результатів.

Очікувана дія: Провести погоджений пілот або моделювання та зафіксувати результати за визначеними критеріями.

Етап 5 Рекомендації і консультаційна взаємодія

Обґрунтування рекомендацій щодо політик доступу, безперервності навчання або цифрового освітнього проєкту відповідно до теми. Оцінювання ресурсів, ризиків та умов перенесення рішення.

Очікувана дія: Підготувати консультаційну записку й обговорити результати з керівником бази.

Етап 6 Звіт і передавання матеріалів дослідження

Систематизація результатів, перевірка простежуваності даних і дотримання конфіденційності. Розмежування фактично виконаного, модельного та запланованого. Підготовка матеріалів для кваліфікаційної роботи.

Очікувана дія: Захистити звіт і пакет матеріалів апробації магістерського дослідження.

5 Тематичний план та розподіл годин для обох форм

Етап	Зміст роботи	Години
Етап 1	Узгодження дослідницького завдання	30
Етап 2	Дослідження об'єкта і ризиків	50
Етап 3	Збирання та підготовка матеріалів	70
Етап 4	Апробація запропонованого рішення	80
Етап 5	Рекомендації і консультаційна взаємодія	70
Етап 6	Звіт і передавання матеріалів дослідження	30
Разом		330

Календарні дати й місця виконання визначаються затвердженим графіком та індивідуальним планом. Керівник погоджує послідовність етапів із урахуванням доступу до аудиторії, даних і ресурсів. Зміни фіксуються у щоденнику або календарі виконання.

6 Практичні завдання та організація виконання

Керівник від Академії погоджує індивідуальне завдання, консультує та перевіряє результати. Для практик керівник від бази організовує дозволену діяльність і надає відгук. Здобувач веде щоденник, своєчасно повідомляє про труднощі й дотримується погоджених правил роботи.

Етап 1 Порядок виконання

Погодити дослідницьке завдання, календар і перелік дозволених матеріалів. Матеріал до звіту: Уточнити протокол дослідження й план управління даними.

Етап 2 Порядок виконання

Побудувати опис об'єкта, реєстр релевантних активів і карту проблем. Матеріал до звіту: Зіставити вихідні умови з обраною моделлю та визначити обмеження.

Етап 3 Порядок виконання

Зібрати дозволені дані або сформулювати погоджений модельний набір із журналом походження. Матеріал до звіту: Підготувати словник даних і протокол перевірки якості.

Етап 4 Порядок виконання

Провести погоджений пілот або моделювання та зафіксувати результати за визначеними критеріями. Матеріал до звіту: Виконати аналіз результатів, похибок і можливих альтернативних пояснень.

Етап 5 Порядок виконання

Підготувати консультаційну записку й обговорити результати з керівником бази. Матеріал до звіту: Уточнити рекомендації з урахуванням зауважень і практичних обмежень.

Етап 6 Порядок виконання

Захистити звіт і пакет матеріалів апробації магістерського дослідження. Матеріал до звіту: Підготувати перелік матеріалів, що передаються до роботи, і план подальшого аналізу.

Мінімальний пакет практики: індивідуальний план; щоденник; паспорт об'єкта; протокол даних; словник або опис матеріалів; обґрунтування методів; результати апробації; аналіз обмежень; консультаційна записка; відгук керівника та звіт. За відсутності дозволу на реальні дані використовується погоджений модельний набір із чітким позначенням статусу.

7 Самостійна робота та індивідуальне завдання

Індивідуальне завдання погоджується з керівником до початку виконання. Воно визначає конкретний об'єкт, результати, етапи, години, доступні матеріали, критерії перевірки й перелік звітних документів. Самостійна підготовка вже включена у 330 годин компонента.

Етап	Самостійно підготовлений матеріал
1	Уточнити протокол дослідження й план управління даними.
2	Зіставити вихідні умови з обраною моделлю та визначити обмеження.
3	Підготувати словник даних і протокол перевірки якості.
4	Виконати аналіз результатів, похибок і можливих альтернативних пояснень.
5	Уточнити рекомендації з урахуванням зауважень і практичних обмежень.
6	Підготувати перелік матеріалів, що передаються до роботи, і план подальшого аналізу.

Щоденник або календар містить дату, виконану дію, витрачені години, посилання на матеріал і позначку погодження керівником. Обсяг фактичної діяльності зіставляється з планом. Матеріали попередніх компонентів можна використовувати як вихідні, але раніше виконані години не зараховуються повторно.

8 Методи навчання та зворотний зв'язок

Наставництво, виконання професійного або дослідницького завдання, спостереження, консультації, обговорення матеріалів, самоаналіз та представлення результатів.

Викладач або керівник надає зворотний зв'язок за критеріями до остаточного подання продукту. Командні справи супроводжуються індивідуальним поясненням внеску. Альтернативний формат подання погоджується за умови перевірки тих самих результатів навчання.

9 Контрольні заходи та критерії оцінювання

Оцінювання здійснюється за 100-бальною шкалою. Наведений розподіл є пропозицією цієї робочої програми для погодження кафедрою, а не твердженням про вже затверджене загальноакадемічне правило. Форми підсумкового контролю відповідають переліку ОК та навчальному плану. До початку навчання здобувач отримує затверджені критерії і розподіл балів.

Критерій	Максимум
Методологічна коректність	25
Дані й простежуваність	30
Апробація та оцінка обмежень	25
Етика і захист звіту	20
Разом	100

Критерій оцінюється за підтвердженими матеріалами. Повний бал відповідає самостійному, коректному й аргументованому виконанню; 75 % максимуму — виконанню з окремими несуттєвими недоліками; 50 % — частковому виконанню з істотними прогалинами; 25 % — фрагментарному результату; 0 — відсутності оцінюваного результату. Проміжні значення визначаються з поясненням недоліків. Загальна оцінка є сумою балів за всіма критеріями.

Звіт і додатки перевіряються разом: для кожного критерію зазначають підтверджувальний матеріал, отриманий бал і пояснення. Відгук керівника бази враховується як джерело доказів; підсумкова оцінка визначається за затвердженою процедурою захисту.

Запитання до захисту

1. Яку освітню проблему розв'язано та як вона пов'язана з інформаційною безпекою?
2. Які матеріали підтверджують особистий внесок і походження даних?
3. Чому обрано саме ці методи й критерії оцінювання?
4. Які педагогічні результати підтверджено і якими доказами?
5. Які обмеження, ризики та альтернативні пояснення враховано?
6. За яких умов результат можна застосувати в іншому освітньому середовищі?

Шкала оцінювання

Бали	ECTS	Екзамен або захист	Залік
90–100	A	Відмінно	Зараховано
80–89	B	Добре	Зараховано
70–79	C	Добре	Зараховано
60–69	D	Задовільно	Зараховано
50–59	E	Задовільно	Зараховано
35–49	FX	Незадовільно; повторне складання	Не зараховано
0–34	F	Незадовільно; повторне вивчення	Не зараховано

Інтервали відтворено за наданими зразками робочих програм. У разі зміни локальної шкали застосовується чинний затверджений акт Академії. Для атестації рішення та можливість повторного проходження визначаються також локальним положенням про атестацію.

10 Організаційні правила та академічна доброчесність

Строки подання робіт і контрольні дати повідомляються на початку компонента. Пропущене заняття або невиконаний етап відпрацьовується шляхом подання рівноцінного продукту та його пояснення. Відвідування саме по собі не є

окремим доказом досягнення результату навчання. У разі об'єктивних перешкод погоджується індивідуальний графік.

До поточного та підсумкового контролю подаються власні роботи з коректними посиланнями. Не допускаються академічний плагіат, фабрикація даних, фальсифікація результатів і привласнення чужого внеску. Перевірка текстових збігів доповнюється змістовним розглядом; автоматичний показник не є самостійним доказом порушення.

Застосування генеративного ШІ допускається лише в межах умов конкретного завдання. Здобувач зазначає інструмент, мету використання, суттєві запити й спосіб перевірки результатів. Заборонено передавати конфіденційні або персональні дані у непогоджені сервіси. Відповідальність за зміст, посилання й висновки несе автор роботи.

Результати попереднього навчання можуть визнаватися відповідно до локальних процедур після зіставлення змісту та результатів. Визнання не замінює обов'язку досягти визначених результатів і не поширюється автоматично на атестацію. Додаткові строки або межі визнання ця програма не встановлює.

Здобувач має право ознайомитися з оціненою роботою, отримати пояснення за критеріями та подати мотивоване звернення про перегляд. Незалежний розгляд, строки й порядок апеляції визначаються чинними локальними актами. На період розгляду зберігаються матеріали роботи та оцінювання.

Доступність забезпечується альтернативними форматами матеріалів, погодженими способами взаємодії й обґрунтованими адаптаціями. Вони мають дозволяти перевірку тих самих результатів навчання. Під час переривання доступу до сервісів використовуються погоджені резервні канали та офлайн-матеріали.

Дослідження інформаційної безпеки здійснюються лише на дозволених навчальних об'єктах. Публічне сканування, перевірка чужих облікових записів та втручання у виробничі системи не входять до навчального завдання. Якщо виявлено ознаки реального інциденту, роботи припиняються, зберігаються наявні матеріали й повідомляється відповідальна особа.

11 Методичне та ресурсне забезпечення

Методичний пакет містить цю програму, навчальні матеріали, інструкції до завдань, приклади оформлення, критерії оцінювання та засоби зворотного зв'язку. Матеріали надаються через погоджений курс Moodle Академії або інший затверджений канал. Адресу конкретного курсу й графік консультацій повідомляє викладач після їх фактичного створення.

Комп'ютер або інший придатний пристрій, доступ до текстового редактора, засобу презентацій, бібліотечних ресурсів і дозволених засобів відеозв'язку. Засоби опрацювання таблиць або локальне аналітичне середовище з фіксацією версій і параметрів.

Викладач перевіряє доступність і працездатність ресурсів до початку завдання. Для кожного програмного засобу визначаються дозволена версія, умови ліцензії та спосіб отримання доступу. Згадування інструмента в програмі не підтверджує його фактичного встановлення; рівноцінна заміна допускається за незмінних результатів навчання.

12 Рекомендовані джерела

Базовими локальними джерелами є ОПП «Професійна освіта. Управління інформаційною безпекою», узгоджений навчальний план 2026 року та чинні положення Академії. Наведені нижче праці й офіційні настанови використовуються для підготовки завдань і самостійної роботи. Повні тексти стандартів ISO опрацьовуються за наявності правомірного доступу; для обов'язкових вправ викладач забезпечує відкриті рівноцінні матеріали.

1. Cohen L., Manion L., Morrison K. Research Methods in Education. 8th ed. Routledge, 2018.

<https://www.routledge.com/Research-Methods-in-Education/CohenManion-Morrison/p/book/9781138209886>

2. British Educational Research Association. Ethical Guidelines for Educational Research. 5th ed., 2024.

<https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-fifth-edition-2024>

3. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024. DOI: 10.6028/NIST.CSWP.29.

<https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>

4. NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. SP 800-61 Rev. 3, 2025. DOI: 10.6028/NIST.SP.800-61r3.

<https://csrc.nist.gov/pubs/sp/800/61/r3/final>

5. UNESCO. Guidance for Generative AI in Education and Research. Paris: UNESCO, 2023.

<https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research>

6. АПСВТ. Методичні рекомендації до проходження переддипломної практики ОК11 за ОПП «Професійна освіта. Управління інформаційною безпекою». Робочі матеріали кафедри інтелектуальних систем та цифрових технологій. Київ, 2026.

Локальні нормативні документи Академії:
<https://www.socosvita.kiev.ua/documents>

Система Moodle Академії: <https://moodle.socosvita.kiev.ua>

13 Організація навчання за формами

Денна і заочна форми мають однакові компетентності, результати навчання, підсумкові продукти та критерії оцінювання. Відрізняється організація навчальної діяльності. Усі завдання й консультації входять до встановленого обсягу компонента.

Для обох форм: 11 ЄКТС, 330 годин; семестр 3. Практики та кваліфікаційна робота не розподіляються за правилом 20 % аудиторних годин дисциплін.

Заочна форма: орієнтир календаря — 8 тижнів практики, 330 годин. Завдання узгоджується з темою кваліфікаційної роботи. Зібрані матеріали можна використовувати в ОК12 із посиланням на походження, без повторного обліку годин.

Практичне завдання за оновленим змістом

Апробувати за темою дослідження педагогічне або управлінське рішення на дозволений базі чи погодженій моделі. Подати протокол походження даних, результати, обмеження й рекомендації; розмежувати впроваджені та модельні результати.

Завдання включається до тематичного портфоліо або індивідуального завдання і оцінюється за відповідною рубрикою цієї програми. Додаткові бали понад 100 за семестр або захист не встановлюються. Оцінювання охоплює особистий внесок, обґрунтованість рішення, якість продукту та пояснення його обмежень.

Зв'язок із вибірковою підготовкою: практикуми ВК22–ВК33 можуть поглиблювати мережеві та кібербезпекові вміння. Вони не є обов'язковою передумовою цього ОК. Основне завдання виконується на доступному навчальному прикладі або погодженій моделі незалежно від вибору дисциплін.