

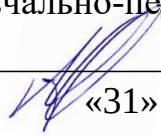
АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

ЗАТВЕРДЖУЮ

Проректор з навчально-педагогічної роботи

—  Ігор ЧОРНОДІД
«31» серпня 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК7

Основи інформаційної безпеки в освітньому середовищі

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: Нізовцев Юрій Юрійович; Кутафін Юрій Володимирович.

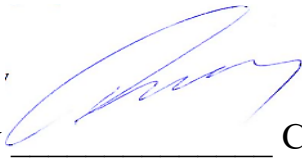
Робочу програму розглянуто на засіданні кафедри інтелектуальних систем та цифрових технологій

Протокол № 1 від «27» серпня 2026 року.

Завідувач кафедри  Ганна КАШИНА

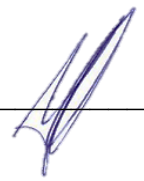
Рекомендовано Вченою радою факультету економіки, соціальних технологій та туризму.

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

© Юрій НІЗОВЦЕВ, Юрій КУТАФІН, 2026 рік

1 Опис освітнього компонента

Показник	Зміст
Статус	Обов'язковий освітній компонент
Обсяг	3 кредити ЄКТС; 90 годин
Семестр	1
Форма контролю	Екзамен
Розподіл годин	Денна: Л 15; Лб 30; СР 45. Заочна: Л 6; Лб 12; СР 72.
Підсумковий продукт	Реєстр активів, модель загроз, план оброблення ризиків і навчальна пам'ятка з кібергігієни.

2 Мета завдання та місце компонента

Сформувати здатність аналізувати інформаційні активи та ризики освітнього середовища, обґрунтовувати політики доступу, приватності й безперервності навчання та організовувати навчання кібергігієни.

Завдання конкретизуються через такі професійні дії: скласти реєстр активів змодельованого закладу та побудувати схему потоків даних; побудувати модель загроз та оцінити п'ять ризиків за явними критеріями; налаштувати рольову модель на дозволеному навчальному стенді та перевірити контрольні сценарії.

2.1 Передумови та наступність

Базова цифрова грамотність, розуміння функцій освітнього середовища та правил роботи з інформацією. Підтримувальні матеріали вирівнюють різний рівень технічної підготовки.

Забезпечує змістові передумови ОК9–ОК12 і безпечне виконання практичних завдань.

3 Заплановані компетентності та результати навчання

Коди й формулювання наведено за матрицями чинної робочої редакції ОПП. 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.
ЗК6	Здатність діяти соціально відповідально та свідомо.
СК3	Здатність застосовувати і створювати нові освітні інструменти і технології та інтегрувати їх в освітнє середовище професійної освіти.
СК4	Здатність аналізувати, прогнозувати, критично осмислювати проблеми у професійній освіті, приймати ефективні рішення щодо їх розв'язання.
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.
СК13	Здатність проєктувати навчання з інформаційної безпеки та кібергігієни, розробляти навчальні матеріали, оцінювати професійні дії здобувачів і надавати консультаційну підтримку учасникам освітнього процесу.
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.
РН7. Створювати освітнє середовище професійної освіти, що є сприятливим для здобувачів освіти і забезпечує досягнення визначених результатів навчання.	Проект або аналіз освітнього середовища з умовами доступності й досягнення результатів.
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.
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.

Результат навчання за ОПП	Доказ у межах компонента
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.
РН17. Розробляти та проводити навчальні заняття і тренінги з інформаційної безпеки та кібергігієни, добирати доступні цифрові засоби, оцінювати практичні дії здобувачів за прозорими критеріями і консультувати учасників освітнього процесу.	Сценарій, матеріали або проведений фрагмент навчання кібергігієни з оцінкою практичних дій.

4 Зміст програми

Тема 1 Активи і межі освітнього середовища

Освітні дані, сервіси, користувачі та інформаційні потоки. Конфіденційність, цілісність і доступність. Власники активів, межі відповідальності та класифікація даних.

Очікувана дія: Скласти реєстр активів змодельованого закладу та побудувати схему потоків даних.

Тема 2 Загрози та оцінювання ризиків

Джерела загроз, вразливості та можливі наслідки для навчання. Критерії ймовірності та впливу, матриця ризику і залишковий ризик. Обмеження якісного оцінювання.

Очікувана дія: Побудувати модель загроз та оцінити п'ять ризиків за явними критеріями.

Тема 3 Ідентифікація та керування доступом

Ролі користувачів, принцип найменших привілеїв, автентифікація й життєвий цикл облікового запису. Відокремлення навчальних і адміністративних повноважень. Документування рішень щодо доступу.

Очікувана дія: Налаштувати рольову модель на дозволеному навчальному стенді та перевірити контрольні сценарії.

Тема 4 Приватність і захист освітніх даних

Мінімізація даних, знеособлення, строки зберігання та правила передавання. Межі використання хмарних сервісів і ІІІ. Етичні наслідки надмірного збирання даних.

Очікувана дія: Проаналізувати форму збору даних і підготувати безпечний варіант навчального набору.

Тема 5 Резервування і реагування на інциденти

Підготовка, виявлення, аналіз, реагування та відновлення. Журнали подій, фіксація часу й збереження вихідних матеріалів. Перевірка резервної копії та пріоритетів відновлення навчання.

Очікувана дія: Виконати навчальне відновлення з резервної копії та оформити протокол сценарію інциденту.

Тема 6 Політики та навчання кібергігієни

План оброблення ризиків, відповідальні особи, контроль виконання та перегляд заходів. Перетворення політики на зрозумілі правила й навчальні вправи. Консультаційна підтримка користувачів.

Очікувана дія: Захистити реєстр активів, модель загроз і план оброблення ризиків; провести мініконсультацію.

5 Тематичний план та розподіл годин денної форми

№	Тема	Л	П	Лб	С	СР	Разом
1	Активи і межі освітнього середовища	3	0	4	0	8	15
2	Загрози та оцінювання ризиків	2	0	6	0	7	15
3	Ідентифікація та керування доступом	3	0	4	0	8	15
4	Приватність і захист освітніх даних	2	0	6	0	7	15
5	Резервування і реагування на інциденти	3	0	4	0	8	15
6	Політики та навчання кібергігієни	2	0	6	0	7	15
Разом		15	0	30	0	45	90

Л — лекції; П — практичні заняття; Лаб — лабораторні заняття; Сем — семінарські заняття; СР — самостійна робота. Обсяг індивідуального завдання, підготовки до контролю й опрацювання джерел враховано у СР. Додаткові години понад план не встановлюються.

6 Практичні завдання та організація виконання денної форми

Завдання лабораторних занять відповідають тематичному плану. Після уточнення умов і критеріїв здобувач виконує завдання, представляє результат та враховує зворотний зв'язок. До портфоліо подаються визначений продукт, коротке обґрунтування й посилання на джерела. Підготовка та доопрацювання входять у години самостійної роботи.

№	Завдання під керівництвом викладача	Продукт до портфоліо	Год.
1	Скласти реєстр активів змодельованого закладу та побудувати схему потоків даних.	Реєстр активів і схема потоків даних.	4
2	Побудувати модель загроз та оцінити п'ять ризиків за явними критеріями.	Модель загроз і матриця ризиків.	6
3	Налаштувати рольову модель на дозволеному навчальному стенді та перевірити контрольні сценарії.	Рольова модель і протокол перевірки доступу.	4
4	Проаналізувати форму збору даних і підготувати безпечний варіант навчального набору.	Знеособлений набір та фрагмент політики.	6
5	Виконати навчальне відновлення з резервної копії та оформити протокол сценарію інциденту.	Протокол відновлення і сценарій інциденту.	4
6	Захистити реєстр активів, модель загроз і план оброблення ризиків; провести мініконсультацію.	План оброблення ризиків і навчальна пам'ятка.	6

7 Самостійна робота та індивідуальне завдання денної форми

Тема	Завдання для самостійного опрацювання	Години
1	Описати межі системи, припущення і пріоритетні освітні сервіси.	8
2	Перевірити чутливість пріоритетів до зміни оцінок впливу.	7
3	Розробити процедуру надання, перегляду й припинення доступу.	8

Тема	Завдання для самостійного опрацювання	Години
4	Написати фрагмент політики приватності для освітнього сервісу.	7
5	Підготувати план ескалації і повідомлення для учасників освітнього процесу.	8
6	Створити пам'ятку з кібергігієни та критерії перевірки практичних дій.	7
Разом		45

7.1 Комплексне індивідуальне завдання

Реєстр активів, модель загроз, план оброблення ризиків і навчальна пам'ятка з кібергігієни.

Об'єкт обирається з трьох рівноцінних варіантів: заклад професійної освіти; фаховий коледж; центр навчання дорослих або корпоративний навчальний підрозділ. Викладач погоджує складність і доступність матеріалів. Можна запропонувати власний об'єкт за однакових вимог до результату.

Завдання виконується поступово в межах тематичної СР: постановка проблеми; пошук та перевірка щонайменше п'яти релевантних джерел; розроблення продукту; обґрунтування рішень; оцінювання обмежень; представлення результату. Підтвердженням є продукт і пояснювальна записка орієнтовно 4–6 сторінок без додатків.

8 Методи навчання та зворотний зв'язок

Проблемне пояснення, аналіз професійних ситуацій, демонстрація, робота з першоджерелами, взаємне рецензування, індивідуальні консультації та рефлексія. Практична робота виконується на ізольованому стенді або з погодженими синтетичними даними; порядок аналізу документується.

Викладач або керівник надає зворотний зв'язок за критеріями до остаточного подання продукту. Командні вправи 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.

Викладачі узгоджують лабораторні завдання, контрольні випадки та рубрики. Кутафін Ю. В. фіксує результати лабораторної роботи; Нізовцев Ю. Ю. забезпечує перевірку фахового змісту й узгодження підсумкового контролю. За один результат бали не нараховуються двічі.

9.1 Семестровий екзамен

Вид роботи	Розрахунок	Максимум
Тематичні навчальні продукти	6×7	42
Дві модульні перевірки	2×8	16
Індивідуальний продукт і пояснення	1×12	12
Екзамен	3×10	30
Разом		100

Для двосеместрових компонентів ця таблиця застосовується до другого семестру. Для односеместрових — до семестру їх вивчення. За кожний тематичний продукт: відповідність завданню — 2; коректність — 2; аргументація — 2; якість подання — 1 бал. Модульна перевірка містить 10 завдань по 0,8 бала. Індивідуальний продукт: обґрунтування — 4; виконання — 4; захист і висновки — 4 бали.

Приклад структури екзаменаційного завдання

1. Ідентифікувати активи, загрози й межі відповідальності у заданому освітньому середовищі. Максимум — 10 балів.

2. Оцінити ризики та обґрунтувати політику доступу, приватності або резервування. Максимум — 10 балів.

3. Представити план реагування й навчальну консультацію для користувача. Максимум — 10 балів.

У кожній частині екзамену оцінюються: коректність змісту — до 4 балів; обґрунтованість рішення — до 3; самостійність відповіді, ясність і пояснення обмежень — до 3. Максимум — 30 балів. Вихідні матеріали й очікувані результати варіантів мають бути рівноцінними.

Питання для підготовки та самоконтролю

1. Як визначити межі освітнього сервісу, його інформаційні активи й власників?
2. Як оцінити ймовірність і наслідки загрози та обґрунтувати пріоритет оброблення ризику?
3. Як перевірити на навчальному стенді принцип найменших привілеїв для різних ролей?
4. Які дані потрібні для навчального завдання та як зменшити ризик ідентифікації учасників?
5. Якими діями й доказами підтвердити працездатність резервної копії та готовність до відновлення?
6. Як перетворити політику інформаційної безпеки на доступну інструкцію і перевірити практичні дії користувача?

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. Тестовий курс або ізольована віртуальна лабораторія з окремими навчальними обліковими записами, синтетичними даними й можливістю відновлення стану.

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. 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>

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

<https://www.iso.org/standard/27001>

3. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

<https://www.iso.org/standard/80585.html>

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. Wazuh Documentation. Навчальне використання засобів аналізу подій безпеки. Офіційна документація.

<https://documentation.wazuh.com/current/index.html>

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

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.

Заочна форма Тематичний план

№	Тема	Л	П	Лб	С	СР	Σ
1	Активи і межі освітнього середовища	1	0	2	0	12	15
2	Загрози та оцінювання ризиків	1	0	2	0	12	15
3	Ідентифікація та керування доступом	1	0	2	0	12	15
4	Приватність і захист освітніх даних	1	0	2	0	12	15
5	Резервування і реагування на інциденти	1	0	2	0	12	15
6	Політики та навчання кібергігієни	1	0	2	0	12	15
	Разом	6	0	12	0	72	90

Л — лекції; П — практичні; Лб — лабораторні; С — семінарські; СР — самостійна робота; Σ — години. Нуль означає відсутність цього виду занять. Розподіл годин між темами є деталізацією навчального плану.

У заочній формі викладач на заняттях пояснює метод і демонструє зразок, організовує виконання ключової дії та перевіряє результат. Підготовка даних, розширене виконання тематичних завдань і доопрацювання портфоліо здійснюються в межах СР за темами. Завдання з розділів практичної та самостійної роботи виконуються за цим погодинним розподілом; наведені там години стосуються денної форми.

Практичне завдання за оновленим змістом

На навчальному прикладі освітньої мережі описати активи, доступи й загрози, обґрунтувати сегментацію, резервування та інструкцію користувачу. Оцінюються модель ризику, достатність заходів і протокол перевірки.

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.