

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 ВИБІРКОВОЇ ДИСЦИПЛІНИ

ВК01

Інформаційна безпека в умовах змішаного навчання

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

Укладач і викладач: Кашина Ганна Сергіївна, доктор педагогічних наук, професор, завідувач кафедри інтелектуальних систем та цифрових технологій.

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

© АПСВТ, 2026 рік

© Ганна КАШИНА, 2026 рік

1 Опис навчальної дисципліни

Показник	Денна форма	Заочна форма
Статус	Вибіркова	Вибіркова
Обсяг	3 кредити ЄКТС / 90 годин	3 кредити ЄКТС / 90 годин
Лекції	10 годин	6 годин
Лабораторні заняття	20 годин	12 годин
Самостійна робота	60 годин	72 години
Практичні та семінарські заняття	Не передбачені	Не передбачені
Підсумковий контроль	Залік	Залік
Змістові модулі	2	2
Семестр	1–3 за індивідуальним планом	1–3 за індивідуальним планом
Рік підготовки	1-й або 2-й відповідно до семестру вибору	1-й або 2-й відповідно до семестру вибору

Розподіл годин відповідає позиції ВК01 каталогу вибірових дисциплін. Підготовка індивідуального проєкту, модульних перевірок і заліку входить до самостійної роботи; додаткові години понад 90 не нараховуються. Частка самостійної роботи денної форми — 66,7 %.

2 Мета завдання та передумови

Мета — сформувати здатність проєктувати та перевіряти безпечно поєднання аудиторного, синхронного й асинхронного навчання, узгоджуючи захист інформації, доступність матеріалів і педагогічну доцільність рішень.

Завдання: визначати інформаційні активи й потоки навчальних даних; оцінювати ризики; установлювати та перевіряти права доступу; організовувати безпечну взаємодію; захищати навчальний контент; планувати відновлення; пояснювати учасникам курсу правила безпечної роботи.

Передумови — базова цифрова грамотність і підготовка попереднього рівня освіти. Поняття ОК7–ОК8 опрацьовуються до відповідних завдань або підтверджуються вхідною діагностикою. Для вибору у першому семестрі передбачено вступне вирівнювання; попереднє завершення інших вибірових дисциплін не є обов'язковим.

3 Компетентності та результати навчання

Дисципліна поглиблює наведені нижче компетентності й результати ОПП. Формулювання відтворено з ОПП; змістові зв'язки ВК01 конкретизовано цією

програмою. Вибір ВК01 не замінює забезпечення обов'язкових результатів обов'язковими компонентами.

Загальні та спеціальні компетентності

ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК3. Здатність застосовувати і створювати нові освітні інструменти і технології та інтегрувати їх в освітнє середовище професійної освіти.

СК10. Здатність ідентифікувати інформаційні активи освітньої організації, оцінювати ризики інформаційної безпеки та обґрунтовувати організаційні й технічні заходи їх оброблення.

СК13. Здатність проєктувати навчання з інформаційної безпеки та кібергігієни, розробляти навчальні матеріали, оцінювати професійні дії здобувачів і надавати консультаційну підтримку учасникам освітнього процесу.

Програмні результати навчання

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.

РН14. Розробляти політики та процедури інформаційної безпеки освітньої організації, визначати правила доступу, оброблення і захисту персональних даних, резервного копіювання та контролю виконання встановлених вимог.

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.

3 Компетентності та результати навчання

Вимірювані результати дисципліни

Код	Результат після завершення дисципліни	Зв'язок з ОПП	Доказ досягнення
РД1	Побудувати карту щонайменше п'яти активів і п'яти потоків навчальних даних та обґрунтувати заходи для трьох пріоритетних ризиків.	ЗК2, СК10; РН13	ЛР1; аналіз ризиків у проєкті
РД2	Скласти матрицю доступу трьох ролей до чотирьох дій і виконати не менше шести перевірок, у тому	СК3, СК10; РН14	ЛР2–ЛР4; протоколи перевірки

	числі двох очікуваних відмов у доступі.		
РД3	Перевірити приватність курсу та відновлення трьох навчальних ресурсів; зіставити результат із вихідними критеріями й зафіксувати обмеження.	ЗК2, СК10; РН13, РН14	ЛР4–ЛР5; модульні ситуації
РД4	Представити інтегровану модель безпечного курсу, провести навчальний фрагмент тривалістю 5–7 хвилин і пояснити власний внесок та результати пілотування.	СК3, СК13; РН17	ЛР6; проєкт і захист

РД — локальні позначення результатів дисципліни, а не нові коди ОПП. Кількісні параметри визначають мінімальний обсяг навчального завдання та не є нормативними вимогами до реальної освітньої системи.

Підсумковий результат навчання

Модель безпечного змішаного курсу з картою доступів, реєстром ризиків, перевіреними налаштуваннями взаємодії, контрольним списком приватності, планом відновлення та навчальною інструкцією для користувачів.

4 Зміст навчальної дисципліни

Змістовий модуль 1 Архітектура і безпечна взаємодія

Тема 1 Межі змішаного освітнього середовища

Аудиторна, синхронна та асинхронна частини курсу; LMS, відеозв'язок, пристрої та домашні підключення. Інформаційні активи, власники, залежності й потоки даних. Конфіденційність, цілісність і доступність у навчальних ситуаціях. Відмежування ризику для навчання від технічної несправності; пріоритезація ризиків за обґрунтованими критеріями [1, 5].

Навчальний результат теми: Карта активів і потоків; три ризики з власниками та заходами оброблення.

Тема 2 Ідентифікація користувачів і розмежування доступу

Життєвий цикл облікового запису: надання, перегляд і відкликання доступу. Автентифікація та авторизація; багатофакторна автентифікація. Контексти й ролі LMS, мінімально необхідні права, доступ викладача, здобувача й гостя. Перевірка очікуваних дозволів і відмов без використання чужих облікових даних [2].

Навчальний результат теми: Матриця доступу та протокол перевірок від імені тестових користувачів.

Тема 3 Безпечна синхронна й асинхронна взаємодія

Керування запрошеннями, посиланнями, гостьовим доступом, демонстрацією екрана та записами занять. Правила форуму, чату, групового завдання й обміну файлами. Розпізнавання підозрілого повідомлення та порядок повідомлення про нього. Узгодження безпеки, доступності й можливостей учасників із нестабільним зв'язком [1, 5].

Навчальний результат теми: Інструкція взаємодії й сценарій онлайн-заняття з перевіреними налаштуваннями.

4 Зміст навчальної дисципліни

Змістовий модуль 2 Приватність, стійкість і педагогічний пілот

Тема 4 Захист даних і навчального контенту

Склад і мінімізація навчальних даних, обґрунтування доступу та строків зберігання. Оцінки, роботи здобувачів, записи зустрічей і журнали подій. Права використання матеріалів та позначення авторства. Перевірка відкритих посилань, зайвих прав і надлишкових даних. Вибір даних для резервної копії; документування змін [2–4, 6].

Навчальний результат теми: Контрольний список приватності з доказами перевірки та виправленнями.

Тема 5 Безперервність навчання та відновлення курсу

Сценарії втрати доступу, помилкового видалення та недоступності платформи. Узгоджені резервні канали комунікації. Вибір складу копії, версій і відповідальної особи. Відновлення лише в тестовій копії та перевірка ресурсів, прав і доступності. Фіксація часу, втрат і обмежень відновлення; повідомлення учасників про зміну порядку навчання [1, 3, 4].

Навчальний результат теми: Протокол відновлення трьох ресурсів і план продовження навчання.

Тема 6 Пілотування безпечного змішаного курсу

Інтеграція налаштувань у педагогічно завершений навчальний фрагмент. Перевірка моделі за ролями та сценаріями. Рубрика безпечної дії, доступна користувачка інструкція, мікротренінг із кібергігієни. Збирання зворотного зв'язку, аналіз помилок і доопрацювання. Особистий внесок, відтворюваність доказів і межі перенесення моделі до реального закладу освіти [1, 5].

Навчальний результат теми: Звіт пілотування, навчальний фрагмент і доопрацьована модель курсу.

5 Тематичний план і розподіл годин

Денна форма навчання

№	Тема	Л	Лб	СР	Усього
1	Межі змішаного освітнього середовища	2	4	9	15
2	Ідентифікація користувачів і розмежування доступу	2	4	9	15
3	Безпечна синхронна й асинхронна взаємодія	2	3	10	15
4	Захист даних і навчального контенту	2	3	10	15
5	Безперервність навчання та відновлення курсу	1	3	11	15
6	Пілотування безпечного змішаного курсу	1	3	11	15
	Разом	10	20	60	90

Заочна форма навчання

№	Тема	Л	Лб	СР	Усього
1	Межі змішаного освітнього середовища	1	2	12	15
2	Ідентифікація користувачів і розмежування доступу	1	2	12	15
3	Безпечна синхронна й асинхронна взаємодія	1	2	12	15
4	Захист даних і навчального контенту	1	2	12	15
5	Безперервність навчання та відновлення курсу	1	2	12	15
6	Пілотування безпечного змішаного курсу	1	2	12	15
	Разом	6	12	72	90

Л — лекції; Лб — лабораторні заняття; СР — самостійна робота.

Кожна тема — 15 годин. Змістовий модуль 1 охоплює теми 1–3, модуль 2 — теми 4–6; кожний модуль становить 45 годин для обох форм навчання.

Розклад і календар подання робіт повідомляються до початку навчання. Для заочної форми самостійна підготовка передуює лабораторним заняттям; аудиторний час використовується для пояснення методу, демонстрації та перевірки ключових дій.

6 Лабораторні заняття

ЛР1 Карта активів і модель ризиків

Тривалість: денна форма — 4 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. Обрати модельний змішаний курс для групи з 20 умовних здобувачів. Описати не менше п'яти активів і п'яти потоків даних між LMS, відеозв'язком, пристроями та сховищем. Для трьох пріоритетних ризиків зазначити причину, наслідок для навчання, оцінку й відповідального.

Звіт і перевірка. Карта потоків, реєстр ризиків і пояснення шкали оцінювання. Перевірка: кожний ризик пов'язано з активом і конкретним заходом.

Ключові критерії. Зв'язки активів і даних; відмежування загрози від вразливості; обґрунтування пріоритету.

ЛР2 Матриця доступу та перевірка ролей

Тривалість: денна форма — 4 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. Підготувати тестові ролі викладача, здобувача та гостя. Побудувати матрицю для перегляду матеріалів, подання роботи, перегляду оцінок і зміни курсу. Перевірити не менше шести комбінацій; дві перевірки мають підтвердити очікувану відмову.

Звіт і перевірка. Матриця «роль × дія», протокол «очікувано / фактично» та знеособлені докази. Перевірка: користувач не отримує зайвих прав.

Ключові критерії. Узгодженість матриці й налаштувань; підтверджені відмови; порядок відкликання доступу.

ЛР3 Безпечне онлайн-заняття

Тривалість: денна форма — 3 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. Побудувати сценарій синхронного заняття з асинхронною альтернативою. Визначити правила запрошення, приєднання гостя, показу екрана, запису й поширення матеріалів. Перевірити один штатний сценарій та один сценарій помилкового поширення посилання.

Звіт і перевірка. Користувацька інструкція, перелік налаштувань і протокол двох сценаріїв. Перевірка: учасник знає дозволені дії та канал повідомлення про проблему.

Ключові критерії. Відповідність освітньому сценарію; безпечний доступ; доступність альтернативного формату.

Звіт містить мету, вихідні умови, виконані дії, докази перевірки, висновок і посилання на використані джерела. Скріншоти мають пояснювальні підписи та не містять паролів або реальних персональних даних.

6 Лабораторні заняття

ЛР4 Перевірка приватності курсу

Тривалість: денна форма — 3 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. На модельних даних перевірити видимість списку учасників, оцінок, поданих робіт, записів і зовнішніх посилань. Визначити надлишкові дані й права. Для кожної невідповідності запропонувати виправлення та повторити перевірку.

Звіт і перевірка. Контрольний список із колонками «об'єкт / ризик / доказ / виправлення / повторна перевірка». Перевірка: немає відкритого доступу до тестових оцінок і робіт.

Ключові критерії. Повнота перевірки; мінімізація даних; доказ усунення помилки.

ЛР5 Резервування та відновлення

Тривалість: денна форма — 3 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. Підготувати тестову копію трьох навчальних ресурсів без реальних персональних даних. Змодельювати втрату доступу або видалення в окремій копії. Відновити ресурси, звірити їхній вміст, доступ і придатність для продовження заняття.

Звіт і перевірка. Протокол зі складом копії, часом виконання, контрольними перевітками та обмеженнями; коротке повідомлення учасникам. Перевірка: усі три ресурси доступні належним ролям.

Ключові критерії. Відтворюваність процедури; перевірені права; обґрунтований резервний канал навчання.

ЛР6 Пілот і навчальний мікротренінг

Тривалість: денна форма — 3 год.; заочна форма — 2 год. Максимальна оцінка тематичного продукту — 8 балів.

Завдання. Провести пілот моделі курсу з тестовими користувачами або рольовою симуляцією. Продемонструвати навчальний фрагмент 5–7 хвилин. Перевірити одну безпечну дію учасника за рубрикою; зібрати зворотний зв'язок і визначити доопрацювання.

Звіт і перевірка. Звіт пілотування, сценарій мікротренінгу, рубрика та журнал змін. Перевірка: зміни впливають із зафіксованих результатів.

Ключові критерії. Педагогічна доцільність; ясність інструкції; перевірка дії; рефлексія результатів.

Звіт містить мету, вихідні умови, виконані дії, докази перевірки, висновок і посилання на використані джерела. Скріншоти мають пояснювальні підписи та не містять паролів або реальних персональних даних.

7 Самостійна робота і заочне навчання

Тема	Зміст самостійної роботи	Денна	Заочна
1	Опрацювати поняття активу, загрози, вразливості й ризику; завершити карту потоків; обґрунтувати шкалу ризиків і джерела даних.	9	12
2	Вивчити ролі та контексти LMS; підготувати тестові облікові записи, матрицю доступу й пояснення результатів перевірки.	9	12
3	Порівняти два варіанти організації взаємодії; підготувати інструкцію, асинхронну альтернативу та відповідь на ситуацію помилкового поширення посилання.	10	12
4	Опрацювати приватність і права використання контенту; заповнити контрольний список; документувати виправлення та повторну перевірку.	10	12
5	Підготувати план резервування й відновлення, опис перевірок і повідомлення учасникам; завершити протокол тестового відновлення.	11	12
6	Інтегрувати матеріали у модель курсу; провести пілот, доопрацювати проєкт, підготувати мікротренінг і відповіді до захисту.	11	12
Разом	Усі завдання, проєкт і підготовка до контролю	60	72

Порядок роботи здобувача заочної форми

До контактних занять здобувач опрацьовує джерела, аналізує кейс і подає попередні матеріали ЛР1–ЛР3. На заняттях демонструє перевірки, отримує зворотний зв'язок і виконує погоджені фрагменти ЛР4–ЛР6. У міжсесійний період завершує звіти та проєкт, проходить дві модульні перевірки за календарем курсу.

Окрема контрольна робота понад передбачені тематичні продукти не вводитьься. Для обох форм однакові результати, обсяг проєкту, максимальні бали

та критерії. Порядок дистанційного захисту визначається розкладом і локальними процедурами Академії.

8 Індивідуальний прикладний проєкт

Модель безпечного змішаного курсу

Об'єкт — один модельний курс закладу професійної освіти, фахового коледжу або навчального центру. Базовий кейс: 20 умовних здобувачів, викладач і запрошений гість; LMS, засіб відеозв'язку та сховище матеріалів. Модель містить три навчальні ресурси й одне завдання з оцінюванням. Вихідні умови можна змінити за погодженням, зберігаючи складність і результати РД1–РД4.

1. Паспорт курсу: мета, аудиторія, способи взаємодії, обмеження доступності та межі моделі.

2. Карта активів і потоків; три пріоритетні ризики, заходи, відповідальні особи та критерії перевірки.

3. Матриця трьох ролей і чотирьох дій; результати позитивних та негативних перевірок.

4. Інструкція безпечної взаємодії; контрольний список приватності; правила доступу до записів і контенту.

5. План резервування та продовження навчання; протокол відновлення трьох ресурсів.

6. Сценарій мікротренінгу, рубрика перевірки дії учасника, результати пілоту та журнал доопрацювань.

7. Висновки про придатність моделі, невирішені обмеження, джерела й декларація особистого внеску.

Матеріали ЛР використовуються як вихідні напрацювання. За 25 балів проєкту оцінюються їх узгоджена інтеграція, доопрацювання та придатність моделі до застосування; повторне подання незмінених звітів не є новим результатом. За ЛР6 оцінюється звіт пілоту, за захист — особиста демонстрація та аргументація.

Рекомендований обсяг пояснювальної записки — 8–12 сторінок без додатків. До неї додаються модель або експорт курсу, інструкції та протоколи. Командна робота допускається з окремим описом і захистом внеску кожного учасника. Усі витрати часу входять до СР.

9 Методи навчання та методичне забезпечення

Проблемне пояснення та аналіз кейсів формують здатність обґрунтовувати рішення; демонстрація й лабораторне виконання — перевіряти їх; навчальне

проектування — інтегрувати педагогічні та безпекові вимоги; взаємне рецензування й рефлексія — виявляти обмеження. Консультації підтримують самостійну роботу та індивідуальну траєкторію.

Метод	Навчальна дія	Доказ
Аналіз освітнього кейсу	Порівняння ризиків і альтернатив	Карта активів та обґрунтування пріоритетів
Демонстрація та лабораторна робота	Налаштування й перевірка ролей, приватності, відновлення	Матриця доступу та протоколи
Навчальне проектування	Створення цілісного змішаного курсу	Проект і навчальна інструкція
Мікровикладання	Пояснення правила й перевірка дії учасника	Мікротренінг і рубрика
Взаємне рецензування	Аналіз доказів і доопрацювання	Відгук та журнал змін

Матеріальне і програмне забезпечення

Комп'ютер або ноутбук із браузером, доступ до інтернету, редактор текстів і таблиць; тестовий курс LMS Moodle або функціонально еквівалентне середовище; дозволений засіб відеозв'язку; тестове сховище та механізм резервування. Права адміністратора всієї платформи здобувачеві не потрібні. Дії, недоступні в ролі викладача, демонструє уповноважений адміністратор або відтворюють у навчальній моделі.

Навчально-методичний комплект

Робоча програма, силабус, анотація, матеріали шести тем, інструкції до ЛР, вихідний кейс, шаблони матриці доступу, реєстру ризиків і протоколів, завдання модульних перевірок, рубрики й джерела. Матеріали та календар доступні через Moodle Академії: <https://moodle.socosvita.kiev.ua>. Посилання на курс і графік консультацій викладач повідомляє перед початком навчання.

10 Контроль і критерії оцінювання

Поточне оцінювання ґрунтується на виконаних діях і доказах результату. Сам факт відвідування не оцінюється балами. Оцінка накопичується за 100-бальною шкалою; окремий екзаме́н не передбачений.

Складова	Кількість і максимум	Разом
Тематичні продукти ЛР1–ЛР6	6 × 8 балів	48
Модульні перевірки М1 і М2	2 × 6 балів	12
Індивідуальний прикладний проєкт	1 × 25 балів	25

Представлення і захист проєкту	1 × 15 балів	15
Загалом		100

Критерії тематичного продукту ЛР

Критерій	Бали	Ознака повного виконання
Виконання вимог	2	Подано всі передбачені елементи завдання.
Коректність рішення	3	Дії й налаштування відповідають кейсу; немає помилок, що спростовують результат.
Перевірка й аргументація	2	Зафіксовано очікуваний і фактичний результат; пояснено обмеження.
Якість документації	1	Звіт зрозумілий, відтворюваний, із джерелами та належно захищеними даними.

Модульні перевірки

М1 охоплює теми 1–3, М2 — теми 4–6. Кожна перевірка містить шість коротких ситуаційних завдань по 1 балу: правильне рішення з належним поясненням — 1; частково правильна відповідь без суттєвої небезпечної дії — 0,5; неправильна відповідь або відсутність — 0. Максимум кожної перевірки — 6 балів.

Для інших критеріїв застосовується частка їх максимуму: 100 % — повне коректне виконання; 75 % — несуттєві недоліки; 50 % — часткове виконання з істотними прогалинами; 25 % — фрагментарний результат; 0 % — результат відсутній або не відповідає завданню. Викладач пояснює виставлені бали.

10 Контроль і критерії оцінювання

Критерії проєкту та захисту

Об'єкт	Критерій	Бали
Проєкт	Аналіз освітнього контексту, ризиків і вимог	5
Проєкт	Узгодженість і коректність цілісної моделі	8
Проєкт	Відтворювані перевірки та аналіз обмежень	5
Проєкт	Педагогічне застосування й доступність	4
Проєкт	Етичність, походження матеріалів і документація	3
Разом за проєкт		25
Захист	Демонстрація працездатності моделі	5
Захист	Обґрунтування рішень і педагогічного застосування	5
Захист	Відповіді на запитання та особистий внесок	5
Разом за захист		15

Підсумкова оцінка

Залік виставляється за сумою накопичених балів. 50–100 балів — «зараховано», 0–49 — «не зараховано». Невиконаний вид роботи оцінюється в 0 балів. Порядок повторного оцінювання та оскарження визначається локальними процедурами Академії [7].

Бали	ECTS	Оцінка для заліку
90–100	A	Зараховано
80–89	B	Зараховано
70–79	C	Зараховано
60–69	D	Зараховано
50–59	E	Зараховано
35–49	FX	Не зараховано; можливість повторного складання
0–34	F	Не зараховано; повторне вивчення дисципліни

11 Орієнтовні контрольні завдання

Приклади модульних ситуацій

М1. Посилання на заняття переслано стороннім особам. Запропонуйте порядок обмеження доступу зі збереженням можливості участі здобувачів. Укажіть, які докази підтвердять результат. Орієнтир відповіді: перевірка складу учасників і налаштувань приєднання, керування гостьовим доступом, погоджений канал повідомлення та повторна перевірка.

М1. Гість курсу бачить оцінки. Визначте актив, порушену властивість безпеки й дію в матриці доступу. Орієнтир: захист конфіденційності оцінок, перегляд ролі в належному контексті та перевірка від імені тестового гостя.

М2. Після відновлення файли відкриваються, але містять застаріле завдання. Поясніть, чому самого факту відкриття недостатньо. Орієнтир: звірення версії й вмісту, придатності до навчальної мети та прав доступу, фіксація обмежень копії.

М2. У скріншот звіту потрапили справжні прізвища й оцінки. Запропонуйте коректний спосіб подання доказу. Орієнтир: використання модельних даних або належне знеособлення, перевірка всіх вкладень і обмеження доступу до матеріалів.

Питання для самоконтролю та захисту

1. Які активи є критичними для продовження обраного курсу і чому?
2. Чим відрізняються автентифікація, авторизація та перевірка доступу?

3. Які дозволи потрібні трьом ролям і як підтверджено відсутність зайвих прав?
4. Як змінюється ризик при відкритому поширенні посилання або запису?
5. Які дані зайві для навчальної мети й як обґрунтовано строки зберігання?
6. Що входить до резервної копії та хто має право її відновлювати?
7. Які три перевірки доводять придатність відновленого курсу?
8. Як забезпечено асинхронну альтернативу й доступність інструкцій?
9. Яку помилку виявив пілот і що змінено після нього?
10. Які межі моделі та умови перенесення до реального закладу освіти?

12 Організаційні умови навчання

Доброчесність та авторський внесок

Здобувач зазначає джерела текстів, зображень, конфігурацій і шаблонів. У звіті відокремлює власні результати від запозичених матеріалів. Використання ШІ декларується: назва засобу, мета, фрагмент роботи та спосіб перевірки. Відповідальність за достовірність висновків і захист даних залишається за автором; конфіденційні матеріали до сторонніх сервісів не передаються.

Безпечне виконання завдань

Перевірки здійснюються лише в тестовому курсі або на погодженому навчальному стенді. Використовуються вигадані чи належно знеособлені дані. Не допускаються зміни прав, видалення даних або перевірки сторонніх ресурсів поза погодженим навчальним завданням. Відновлення виконується в окремій копії; робочу освітню систему не використовують для моделювання відмови.

Подання доопрацювання та зворотний зв'язок

Календар, канал подання, формати файлів і консультації оприлюднюються до початку курсу. Пропущене заняття відпрацьовується рівноцінним завданням із демонстрацією результату. Порядок подання робіт після переривання навчання узгоджується в межах локальних процедур. Доопрацювання подається з журналом змін; зауваження викладача співвідносяться з оголошеними критеріями.

Доступність та індивідуальна траєкторія

За потреби погоджуються доступний формат матеріалів, асинхронний спосіб демонстрації, альтернативний цифровий інструмент або рольова модель перевірки. Альтернатива має підтверджувати ті самі результати РД1–РД4 і оцінюється за однаковими критеріями. Технічні обмеження та погоджені зміни фіксуються до виконання завдання.

13 Рекомендовані джерела та інформаційні ресурси

Основні джерела

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024. DOI: 10.6028/NIST.CSWP.29. URL: <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>
2. Moodle Documentation. Roles and permissions. Moodle 4.5 documentation. URL: https://docs.moodle.org/405/en/Roles_and_permissions
3. Moodle Documentation. Course backup. Moodle 4.5 documentation. URL: https://docs.moodle.org/405/en/Course_backup
4. Moodle Documentation. Course restore. Moodle 4.5 documentation. URL: https://docs.moodle.org/405/en/Course_restore
5. Redecker C. European Framework for the Digital Competence of Educators: DigCompEdu / ed. Y. Punie. Luxembourg: Publications Office of the European Union, 2017. DOI: 10.2760/159770. URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC107466>
6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (редакцію перевіряють на дату виконання завдання).
7. Академія праці, соціальних відносин і туризму. Положення про організацію освітнього процесу. 2026. Розділи щодо робочих програм і оцінювання; додаток 6. Електронна копія: [educational-process-2026.pdf](#).
8. Академія праці, соціальних відносин і туризму. Освітньо-професійна програма «Професійна освіта. Управління інформаційною безпекою». Доопрацьований проєкт, 2026. Розділи щодо компетентностей і результатів навчання.
9. Академія праці, соціальних відносин і туризму. Каталог вибірових дисциплін ВК01–ВК33. 2026. Позиція ВК01.

Використання ресурсів

Джерела [1–6] використовуються для аналізу й виконання навчальних завдань; [7–9] визначають організаційні та програмні орієнтири. Для Moodle застосовується документація встановленої версії; конкретні назви елементів інтерфейсу можуть відрізнятися. Дата перевірки електронних навчальних ресурсів [1–5] — 18.08.2026. Законодавчі положення перевіряються за офіційним текстом на дату застосування.

Інформаційне середовище дисципліни: Moodle Академії —
<https://moodle.socosvita.kiev.ua>.