

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

СИЛАБУС

ВК01 Інформаційна безпека в умовах змішаного навчання

ОПП «Професійна освіта. Управління інформаційною безпекою»

Магістр • А5 Професійна освіта (за спеціалізаціями) • А Освіта

Денна та заочна форми навчання • Київ 2026

Показник	Зміст
Статус і обсяг	Вибірковий компонент; 3 ЄКТС; 90 годин
Семестр і контроль	1–3 за індивідуальним планом; Залік
Викладачі або керівники	Кашина Ганна Сергіївна
Денна форма	Л 10; Лб 20; СР 60
Заочна форма	Л 6; Лб 12; СР 72

Мета та передумови

Сформувати здатність проектувати та перевіряти безпечне поєднання аудиторного, синхронного й асинхронного навчання, узгоджуючи захист інформації, доступність матеріалів і педагогічну доцільність рішень.

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.

Мова викладання — українська. Контакти викладачів, календар занять і графік консультацій повідомляються перед початком навчання.

Тематичний план і навантаження

№	Навчальна тема	Денна	Заочна	Усього
1	Межі змішаного освітнього середовища	2/4/9	1/2/12	15
2	Ідентифікація користувачів і розмежування доступу	2/4/9	1/2/12	15
3	Безпечна синхронна й асинхронна взаємодія	2/3/10	1/2/12	15
4	Захист даних і навчального контенту	2/3/10	1/2/12	15
5	Безперервність навчання та відновлення курсу	1/3/11	1/2/12	15
6	Пілотування безпечного змішаного курсу	1/3/11	1/2/12	15
	Разом	10/20/60	6/12/72	90

Години у стовпцях «Денна» і «Заочна» наведено в порядку Л / Лб / СР.

Л — лекції; П — практичні заняття; Лб — лабораторні; С — семінарські; СР — самостійна робота. Усього — години теми для кожної форми окремо.

Компетентності та результати навчання

Компетентності за програмою: ЗК2, СКЗ, СК10, СК13.

Вибірковий компонент поглиблює зазначені результати ОПП. Його вибір не замінює забезпечення обов'язкових результатів обов'язковими компонентами.

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.

Вимірювані результати дисципліни

РД1. Побудувати карту щонайменше п'яти активів і п'яти потоків навчальних даних та обґрунтувати заходи для трьох пріоритетних ризиків.

РД2. Скласти матрицю доступу трьох ролей до чотирьох дій і виконати не менше шести перевірок, у тому числі двох очікуваних відмов у доступі.

РД3. Перевірити приватність курсу та відновлення трьох навчальних ресурсів; зіставити результат із вихідними критеріями й зафіксувати обмеження.

РД4. Представити інтегровану модель безпечного курсу, провести навчальний фрагмент тривалістю 5–7 хвилин і пояснити власний внесок та результати пілотування.

Навчальні завдання та підсумковий продукт

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

1. Побудувати карту щонайменше п'яти активів і п'яти потоків навчальних даних; обґрунтувати заходи для трьох пріоритетних ризиків.

2. Скласти матрицю трьох ролей і чотирьох дій; виконати шість перевірок доступу, зокрема дві перевірки очікуваної відмови.

3. Підготувати сценарій безпечного онлайн-заняття з асинхронною альтернативою та протоколом перевірки налаштувань.

4. Перевірити видимість оцінок, робіт, записів і посилань на модельних даних; оформити контрольний список приватності.

5. Відновити три навчальні ресурси у тестовій копії; перевірити їх доступність і права користувачів.

6. Провести пілот курсу й мікротренінг; подати зворотний зв'язок, рубрику оцінювання та журнал доопрацювань.

Матеріали портфоліо або звіту містять вихідні умови, виконані дії, перевірку результату, висновки та посилання. Завдання виконуються в межах установлених годин; підготовка до контролю не додається понад обсяг компонента.

Заочна форма: попередня підготовка й опрацювання матеріалів відбуваються самостійно; на заняттях викладач пояснює метод, демонструє ключові дії, перевіряє виконання та надає зворотний зв'язок. Підсумкові результати й критерії відповідають денній формі.

Контроль і критерії оцінювання

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

Складова	Кількість і максимум	Разом
Представлення і захист проєкту	1 × 15 балів	15
Загалом		100

Тематичний продукт — 8 балів: виконання вимог 2, коректність 3, перевірка й аргументація 2, документація 1. Кожна модульна перевірка містить шість завдань по 1 балу.

Прикладний проєкт — 25 балів: аналіз 5, якість рішення 8, перевірка 5, педагогічне застосування 4, етичність і документування 3. Захист — 15 балів: демонстрація, обґрунтування, відповіді й особистий внесок — по 5 балів.

Кожний критерій: повне коректне виконання — 100 % максимуму; неістотні недоліки — 75 %; істотні прогалини — 50 %; фрагментарний результат — 25 %; відсутній результат — 0. Проміжні бали супроводжуються поясненням.

Шкала: 90–100 — А; 80–89 — В; 70–79 — С; 60–69 — D; 50–59 — Е; 35–49 — FХ; 0–34 — F. Залік: 50–100 — зараховано. Критерії однакові для обох форм навчання; перед початком компонента оприлюднюють затверджений порядок оцінювання.

Організація навчання та джерела

Навчання поєднує пояснення, аналіз кейсів, практичні або лабораторні дії відповідно до плану, проєктування, консультації, взаємне рецензування та рефлексію.

Строки подання робіт і консультацій визначає календар компонента. Пропущене завдання відпрацьовується рівноцінним продуктом. Альтернативні формати й обґрунтовані адаптації мають дозволяти перевірку тих самих результатів. Здобувач отримує пояснення оцінки та може звернутися щодо її перегляду за локальними процедурами Академії.

Роботи виконуються самостійно, з посиланнями на джерела та підтвердженням особистого внеску. Використання генеративного ШІ декларується; результати перевіряються автором. Для навчальних перевірок використовуються погоджені тестові об'єкти й модельні дані.

Ресурсне 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.

Рекомендовані 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

Документи ОПП та чинні локальні положення Академії: <https://www.socosvita.kiev.ua/documents>. Навчальні матеріали й консультації — через погоджений канал курсу Moodle: <https://moodle.socosvita.kiev.ua>.