АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

СИЛАБУС

ВК28 Безпека хмарних сервісів і контейнерів: лабораторний практикум

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	Брезецький Сергій Олександрович
Денна форма	Л 10; Лб 30; СР 50
Заочна форма	Л 6; Лб 12; СР 72

Мета та передумови

Перевіряти конфігурацію доступу, секретів і відновлення навчальних хмарних сервісів.

Передумови. базова цифрова грамотність і підготовка попереднього рівня освіти. Профільні поняття ОК7–ОК8 опрацьовуються до відповідного завдання або підтверджуються вхідною діагностикою. Інші вибіркові дисципліни не встановлюються обов’язковою умовою доступу.

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

Тематичний план і навантаження

№	Навчальна тема	Денна	Заочна	Усього
1	Архітектура й відповідальність	2/5/8	1/2/12	15
2	Доступ і облікові ролі	2/5/8	1/2/12	15
3	Секрети й конфігурація	2/5/8	1/2/12	15
4	Ізоляція контейнера	2/5/8	1/2/12	15
5	Журнали та відновлення	1/5/9	1/2/12	15
6	Навчальний сценарій	1/5/9	1/2/12	15
	Разом	10/30/50	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, СК3, СК10, СК11.

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

РН2. Ефективно використовувати сучасні цифрові інструменти, інформаційні технології та ресурси у професійній, інноваційній та/або дослідницькій діяльності.

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.

Вимірювані результати дисципліни

РД1. Описати об’єкт і вихідні дані, визначити щонайменше три критерії якості рішення та обґрунтувати їх освітню доцільність.

РД2. Виконати шість тематичних завдань, подати результати та відтворювані докази виконання за завданнями цього силабуса.

РД3. Перевірити рішення за визначеними критеріями; зіставити очікувані та фактичні результати щонайменше двох перевірок і пояснити обмеження.

РД4. Інтегрувати результати у прикладний продукт, представити його освітнє застосування й захистити особистий внесок.

Навчальні завдання та підсумковий продукт

Підсумковий продукт. Конфігурація сервісу, модель доступу й звіт перевірки

1. Побудувати схему відповідальності навчального сервісу.
2. Налаштувати та перевірити ролі користувачів.
3. Перевірити тестову конфігурацію на небезпечне зберігання секретів.
4. Запустити контейнер із погодженим профілем обмежень.
5. Відновити навчальний сервіс та оформити протокол.
6. Захистити сервіс і лабораторну інструкцію.

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	6 × 8 балів	48
Модульні перевірки M1 і M2	2 × 6 балів	12
Індивідуальний прикладний проєкт	1 × 25 балів	25
Представлення і захист	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 — A; 80–89 — B; 70–79 — C; 60–69 — D; 50–59 — E; 35–49 — FX; 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

Локальний контейнерний стенд або погоджене навчальне хмарне середовище.

Рекомендовані джерела

1. Docker. Docker Engine Security. Офіційна документація. https://docs.docker.com/engine/security/

2. 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

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Редакцію перевіряють на дату застосування. https://zakon.rada.gov.ua/laws/show/2297-17

4. Canonical. Ubuntu Server Documentation. Security. Офіційна документація. https://documentation.ubuntu.com/server/

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.