

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

СИЛАБУС

ОК05 Стратегічний менеджмент у сфері професійної освіти

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	Обов'язковий компонент; 3 кредити ЄКТС; 90 годин
Семестр і контроль	1; Екзамен
Викладачі або керівники	Любарець Владислава Вікторівна
Денна форма	Л 30; П 15; Лб 0; С 0; СР 45
Заочна форма	Л 12; П 6; Лб 0; С 0; СР 72

Мета та передумови

Сформувати здатність обґрунтовувати стратегію безпечного цифрового розвитку освітньої організації, узгоджувати цілі, ресурси й відповідальність, управляти командою та оцінювати результати змін.

Передумови. Базові уявлення про організацію освітнього процесу, командну діяльність та цифрові ресурси. Інформаційно-безпекові приклади узгоджуються з паралельним вивченням ОК7.

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

Тематичний план і навантаження

№	Навчальна тема	Денна	Заочна	Усього
1	Стратегічний аналіз освітньої організації	5/3/7	2/1/12	15
2	Цілі та альтернативи розвитку	5/2/8	2/1/12	15
3	Ресурси і відповідальність	5/3/7	2/1/12	15
4	Управління змінами і командою	5/2/8	2/1/12	15
5	Безпека та безперервність як стратегічні завдання	5/3/7	2/1/12	15
6	Моніторинг і перегляд стратегії	5/2/8	2/1/12	15
	Разом	30/15/45	12/6/72	90

Години у стовпцях «Денна» і «Заочна» наведено в порядку Л / П / 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: ІК, ЗК1, ЗК3, ЗК5, ЗК6, СК4, СК5, СК6, СК8, СК11, СК14.

РН1. Знати на рівні новітніх досягнень основні концепції сталого розвитку суспільства, освіти і методології наукового пізнання у сфері професійної освіти.

РН5. Обирати оптимальну стратегію колективної діяльності, міжособистісного спілкування та взаємодії для реалізації комплексних проєктів у професійній освіті та міждисциплінарних проєктів з урахуванням етичних, правових, соціальних та економічних аспектів.

РН11. Проєктувати та впроваджувати освітні й цифрові рішення відповідно до принципів сталого розвитку, цифрової екології та універсального дизайну, забезпечуючи їх соціальну відповідальність, доступність та інклюзивність.

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

РН16. Проєктувати та реалізовувати цифровий освітній проєкт із визначеними вимогами до інформаційної безпеки, керувати командною взаємодією, ресурсами і ризиками та оцінювати педагогічну й організаційну результативність проєкту.

Навчальні завдання та підсумковий продукт

Підсумковий продукт. Стратегічний план безпечного цифрового розвитку освітньої організації.

1. Стратегічний аналіз і карта стейкхолдерів.
2. Матриця альтернатив і дерево цілей.
3. Ресурсний план, бюджет і матриця відповідальності.
4. Протокол обговорення і план комунікацій.
5. Політика безпеки та сценарій безперервності.
6. Стратегічний план і система показників.

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

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

Тематичний продукт — 7 балів: відповідність завданню 2, коректність 2, аргументація 2, якість подання 1. Індивідуальний продукт — 12 балів: обґрунтування, виконання, захист і висновки — по 4. Модульна перевірка — 10 завдань по 0,8 бала.

Екзамен: три завдання по 10 балів. За кожне завдання оцінюються коректність і повнота — 4, обґрунтування — 3, самостійність та якість представлення — 3.

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 інший придатний пристрій, доступ до текстового редактора, засобу презентацій, бібліотечних ресурсів і дозволених засобів відеозв'язку.

Рекомендовані джерела

1. ISO 21502:2020. Project, programme and portfolio management — Guidance on project management. <https://www.iso.org/standard/74947.html>

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. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. <https://www.iso.org/standard/80585.html>

4. Redecker C. European Framework for the Digital Competence of Educators: DigCompEdu. European Commission, Joint Research Centre, 2017. DOI: 10.2760/159770. <https://publications.jrc.ec.europa.eu/repository/handle/JRC107466>

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>.