

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

СИЛАБУС

ВК02 Менеджмент інцидентів інформаційної безпеки в освіті

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	Нізовцев Юрій Юрійович
Денна форма	Л 20; П 10; СР 60
Заочна форма	Л 12; П 6; СР 72

Мета та передумови

Організовувати виявлення, координацію реагування та відновлення освітніх 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	Класифікація інцидентів	4/2/9	2/1/12	15
2	Підготовка реагування	4/2/9	2/1/12	15
3	Первинний аналіз	3/2/10	2/1/12	15
4	Локалізація та відновлення	3/2/10	2/1/12	15
5	Комунікація й документація	3/1/11	2/1/12	15
6	Сценарна вправа	3/1/11	2/1/12	15
	Разом	20/10/60	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: ЗКЗ, СК11, СК12, СК14.

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

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

РН15. Аналізувати дані про кіберінциденти, документувати висновки, визначати пріоритети реагування та план відновлення цифрових освітніх сервісів, оцінювати обмеження й похибки інструментів штучного інтелекту.

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.

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. Регламент реагування і пакет документів навчального інциденту

1. Класифікувати шість навчальних подій і пояснити пріоритети.
2. Розробити матрицю відповідальності і схему повідомлень.
3. Скласти часову шкалу модельного інциденту.
4. Порівняти два сценарії відновлення освітнього сервісу.
5. Підготувати картку інциденту й повідомлення навчальній групі.
6. Провести настільну вправу та захистити план удосконалення.

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 — 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

Текстовий і табличний редактори, Moodle, навчальні кейси та погоджене середовище демонстрації.

Рекомендовані джерела

1. 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>

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>.