

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

Кафедра інтелектуальних систем та цифрових технологій

СИЛАБУС

ОК07 Основи інформаційної безпеки в освітньому середовищі

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	Нізовцев Юрій Юрійович; Кутафін Юрій Володимирович
Денна форма	Л 15; П 0; Лб 30; С 0; СР 45
Заочна форма	Л 6; П 0; Лб 12; С 0; СР 72

Мета та передумови

Сформувати здатність аналізувати інформаційні активи та ризики освітнього середовища, обґрунтовувати політики доступу, приватності й безперервності навчання та організовувати навчання кібергігієни.

Передумови. Базова цифрова грамотність, розуміння функцій освітнього середовища та правил роботи з інформацією. Підтримувальні матеріали вирівнюють різний рівень технічної підготовки.

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

Тематичний план і навантаження

№	Навчальна тема	Денна	Заочна	Усього
1	Активи і межі освітнього середовища	3/4/8	1/2/12	15
2	Загрози та оцінювання ризиків	2/6/7	1/2/12	15
3	Ідентифікація та керування доступом	3/4/8	1/2/12	15
4	Приватність і захист освітніх даних	2/6/7	1/2/12	15
5	Резервування і реагування на інциденти	3/4/8	1/2/12	15
6	Політики та навчання кібергігієни	2/6/7	1/2/12	15
	Разом	15/30/45	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: ІК, ЗК1, ЗК2, ЗК6, СК3, СК4, СК7, СК9, СК10, СК11, СК13, СК14.

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

РН7. Створювати освітнє середовище професійної освіти, що є сприятливим для здобувачів освіти і забезпечує досягнення визначених результатів навчання.

РН10. Здійснювати консультативну діяльність у сфері професійної освіти.

РН12. Дотримуватися принципів академічної доброчесності та цифрової етики, відповідально використовувати цифрові технології й штучний інтелект, забезпечувати прозорість, безпеку та етичне управління освітніми даними.

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.

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

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.

Навчальні завдання та підсумковий продукт

Підсумковий продукт. Реєстр активів, модель загроз, план оброблення ризиків і навчальна пам'ятка з кібергігієни.

1. Реєстр активів і схема потоків даних.
2. Модель загроз і матриця ризиків.
3. Рольова модель і протокол перевірки доступу.
4. Знеособлений набір та фрагмент політики.
5. Протокол відновлення і сценарій інциденту.
6. План оброблення ризиків і навчальна пам'ятка.

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. Тестовий курс або ізольована віртуальна лабораторія з окремими навчальними обліковими записами, синтетичними даними й можливістю відновлення стану.

Рекомендовані джерела

1. 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>

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. <https://www.iso.org/standard/27001>

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. 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>

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>.