

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Факультет економіки, соціальних технологій та туризму

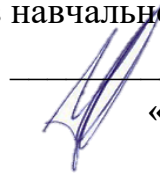
Кафедра інтелектуальних систем та цифрових технологій

ЗАТВЕРДЖУЮ

Проректор з навчально-педагогічної роботи

Ігор ЧОРНОДІД

«31» серпня 2026 року



РОБОЧА ПРОГРАМА ВИБІРКОВОЇ ДИСЦИПЛІНИ

ВК23

Мережева кібербезпека за технологіями Cisco: лабораторний практикум

Освітньо-професійна програма

«Професійна освіта. Управління інформаційною безпекою»

Другий (магістерський) рівень вищої освіти

Спеціальність А5 Професійна освіта (за спеціалізаціями)

Галузь знань А Освіта

Денна та заочна форми навчання

Мова викладання — українська

Київ 2026

Відомості про розроблення і погодження

Укладач і викладач: Кутафін Юрій Володимирович.

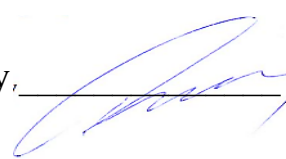
Робочу програму розглянуто на засіданні кафедри інтелектуальних систем та цифрових технологій

Протокол № 1 від «27» серпня 2026 року.

Завідувач кафедри  Ганна КАШИНА

Рекомендовано Вченою радою факультету економіки, соціальних технологій та туризму.

Протокол № 1 від «27» серпня 2026 року.

Декан факультету,  Сергій ШОЛУДЧЕНКО

Схвалено науково-методичною радою Академії

Протокол № 1 від «31» серпня 2026 року.

Голова ради  Ігор ЧОРНОДІД

© АПСВіТ, 2026 рік

© Юрій КУТАФІН, 2026 рік

1 Опис навчальної дисципліни

Показник	Денна форма	Заочна форма
Статус	Вибіркова	Вибіркова
Обсяг	3 кредити ЄКТС / 90 годин	3 кредити ЄКТС / 90 годин
Лекції	10 годин	6 годин
Лабораторні заняття	30 годин	12 годин
Самостійна робота	50 годин	72 годин
Підсумковий контроль	Залік	Залік
Змістові модулі	2	2
Семестр	1–3 за індивідуальним планом	1–3 за індивідуальним планом
Рекомендований семестр	2–3	2–3

Кожний змістовий модуль становить 45 годин: модуль 1 — теми 1–3, модуль 2 — теми 4–6. Підготовка проєкту, модульних перевірок і заліку входить до самостійної роботи. Додаткові години понад 90 не нараховуються.

2 Мета, завдання та передумови

Перевіряти мережеві правила доступу та захищену конфігурацію навчальної мережі Cisco. Дисципліна поглиблює індивідуальну підготовку магістра професійної освіти; технічні й управлінські дії пов'язуються з безпечним навчанням та педагогічним використанням результату.

Завдання: засвоїти поняття та методи дисципліни; обґрунтовувати рішення в освітньому контексті; виконувати тематичні завдання з документуванням доказів; інтегрувати результати у прикладний продукт і пояснювати їх педагогічне застосування.

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.

Рекомендація вивчати у 2–3 семестрах пов'язана з потребою у попередніх профільних умінях. Вибір у першому семестрі можливий за підтвердженої еквівалентної підготовки та організаційної можливості.

Перед початком технічних завдань перевіряються навички роботи з обліковими записами, файлами, базовими мережевими параметрами та

погодженим навчальним середовищем. Потрібні уміння уточнюються за вхідною вправою.

3 Компетентності та результати навчання

Дисципліна поглиблює наведені компетентності та результати ОПП. Їх формулювання відтворено з ОПП; вибір дисципліни не замінює забезпечення обов'язкових результатів обов'язковими освітніми компонентами.

Загальні та спеціальні компетентності

ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК10. Здатність ідентифікувати інформаційні активи освітньої організації, оцінювати ризики інформаційної безпеки та обґрунтовувати організаційні й технічні заходи їх оброблення.

СК11. Здатність розробляти, впроваджувати й оцінювати політики та процедури управління інформаційною безпекою цифрового освітнього середовища з урахуванням вимог законодавства і захисту персональних даних.

СК13. Здатність проектувати навчання з інформаційної безпеки та кібергігієни, розробляти навчальні матеріали, оцінювати професійні дії здобувачів і надавати консультаційну підтримку учасникам освітнього процесу.

Програмні результати навчання

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

Код	Результат дисципліни	Зв'язок з ОПП	Доказ
-----	----------------------	---------------	-------

Код	Результат дисципліни	Зв'язок з ОПП	Доказ
РД1	Описати об'єкт і вихідні дані, визначити щонайменше три критерії якості рішення та обґрунтувати їх освітню доцільність.	ЗК2, СК10; РН13	Тематичні завдання 1–2
РД2	Виконати шість тематичних завдань, подати результати та відтворювані докази виконання відповідно до розділу 6.	СК10, СК11, СК13; РН13, РН14, РН17	Продукти тем 1–6
РД3	Перевірити рішення за визначеними критеріями; зіставити очікувані та фактичні результати щонайменше двох перевірок і пояснити обмеження.	СК13; РН14, РН17	Протоколи перевірки; модулі
РД4	Інтегрувати результати у прикладний продукт, представити його освітнє застосування й захистити особистий внесок.	СК11, СК13; РН17	Проект і захист

РД — локальні позначення результатів дисципліни. Кількісні параметри визначають обсяг навчального завдання. Підсумковий продукт: Захищена модель мережі, матриця доступу й протокол тестування.

4 Зміст навчальної дисципліни

Змістовий модуль 1. Концептуальні засади та початкові рішення

Тема 1. Вимоги мережевого захисту

Активи, довірчі межі, користувацькі ролі й допустимі потоки даних.

Очікувана професійна дія: Підготувати модель загроз і матрицю потоків.

Тема 2. Сегментація мережі

Навчальні, адміністративні та гостьові сегменти; обмеження взаємодії.

Очікувана професійна дія: Спроектувати й перевірити сегментацію стенду.

Тема 3. Правила контролю доступу

Дозволені з'єднання, порядок правил, мінімальні права та контрольні сценарії.

Очікувана професійна дія: Налаштувати списки доступу і виконати позитивні та негативні тести.

Змістовий модуль 2. Перевірка, інтеграція і професійне застосування

Тема 4. Адміністративне керування

Захищений доступ, облікові ролі, збереження конфігурацій і журналювання.

Очікувана професійна дія: Перевірити доступ адміністратора й відмову неповноважній ролі.

Тема 5. Захист комутації та події

Доступні механізми захисту портів, журнали й межі підтримки симулятора.

Очікувана професійна дія: Перевірити погоджену конфігурацію та задокументувати обмеження.

Тема 6. Тренінг безпечної конфігурації

Пояснення типових помилок, контрольний список і методичне оцінювання.

Очікувана професійна дія: Захистити модель і провести фрагмент тренінгу.

5 Тематичний план і розподіл годин

Денна форма навчання

№	Тема	Л	Лб	СР	Усього
1	Вимоги мережевого захисту	2	5	8	15
2	Сегментація мережі	2	5	8	15
3	Правила контролю доступу	2	5	8	15
4	Адміністративне керування	2	5	8	15
5	Захист комутації та події	1	5	9	15
6	Тренінг безпечної конфігурації	1	5	9	15
	Разом	10	30	50	90

Заочна форма навчання

№	Тема	Л	Лб	СР	Усього
1	Вимоги мережевого захисту	1	2	12	15

№	Тема	Л	Лб	СР	Усього
2	Сегментація мережі	1	2	12	15
3	Правила контролю доступу	1	2	12	15
4	Адміністративне керування	1	2	12	15
5	Захист комутації та події	1	2	12	15
6	Тренінг безпечної конфігурації	1	2	12	15
	Разом	6	12	72	90

Л — лекції; П — практичні заняття; Лб — лабораторні заняття; С — семінарські заняття; СР — самостійна робота. Розподіл між темами деталізує загальний обсяг дисципліни. Календар занять і подання робіт повідомляється до початку навчання.

6 Навчальні заняття та завдання

Усі шість занять утворюють послідовність роботи над одним модельним об'єктом. За кожний тематичний продукт можна отримати до 8 балів. Виконання на занятті та самостійне доопрацювання разом формують один продукт, який оцінюється один раз.

Лабораторна робота 1. Вимоги мережевого захисту

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Підготувати модель загроз і матрицю потоків. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

Лабораторна робота 2. Сегментація мережі

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Спроекувати й перевірити сегментацію стенду. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

Лабораторна робота 3. Правила контролю доступу

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Налаштувати списки доступу і виконати позитивні та негативні тести. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

Лабораторна робота 4. Адміністративне керування

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Перевірити доступ адміністратора й відмову неповноважній ролі. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

Лабораторна робота 5. Захист комутації та події

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Перевірити погоджену конфігурацію та задокументувати обмеження. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

Лабораторна робота 6. Тренінг безпечної конфігурації

Аудиторний час: денна форма — 5 год.; заочна форма — 2 год.

Завдання: Захистити модель і провести фрагмент тренінгу. Визначити вихідні умови, пояснити спосіб виконання та додати матеріали, за якими можна перевірити результат.

Звіт і перевірка: подати тематичний продукт, короткий опис виконаних дій та зіставлення очікуваного й фактичного результату. Зафіксувати джерело вихідних матеріалів, виявлені обмеження та запропоноване доопрацювання.

Критерії: відповідність завданню теми; коректність методу; достатність доказів; зрозумілість документації. Розподіл 8 балів наведено в розділі 10.

7 Самостійна робота і заочне навчання

Тема	Зміст самостійної роботи	Денна	Заочна
1	Підготувати модель загроз і матрицю потоків. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	8	12
2	Спроектувати й перевірити сегментацію стенду. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	8	12
3	Налаштувати списки доступу і виконати позитивні та негативні тести. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	8	12
4	Перевірити доступ адміністратора й відмову неповноважній ролі. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	8	12
5	Перевірити погоджену конфігурацію та задокументувати обмеження. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	9	12
6	Захистити модель і провести фрагмент тренінгу. Опрацювати профільні джерела; завершити та перевірити матеріали теми.	9	12
Разом	Тематичні завдання, проєкт і підготовка до контролю	50	72

У межах зазначених годин здобувач готує тематичні продукти, інтегрує прикладний проєкт, виконує модульні перевірки та готується до захисту. Обсяг СР денної форми — 50 год.; заочної — 72 год.

Порядок роботи здобувача заочної форми

До контактних занять опрацювати поняття й вихідні матеріали тем 1–3 та подати попередні результати. На заняттях продемонструвати ключові дії, отримати зворотний зв'язок і погодити спосіб перевірки. У міжсесійний період завершити шість продуктів, виконати дві модульні перевірки та інтегрувати проєкт.

Окрема контрольна робота понад зазначені завдання не вводиться. Результати, склад проєкту, максимальні бали та критерії для обох форм однакові. Дистанційне подання і захист організовуються за календарем курсу та локальними процедурами Академії.

8 Індивідуальний прикладний проєкт

Захищена модель мережі, матриця доступу й протокол тестування

Об'єкт — модельний заклад професійної освіти, фаховий коледж, навчальний центр або його цифровий сервіс. Конкретний кейс узгоджується до виконання завдань. Використовуються вигадані чи належно знеособлені дані. Підсумковий пакет включає:

Паспорт об'єкта: проблема, аудиторія, вихідні умови, межі та критерії результату.

Матеріали шести тем із поясненням їх взаємозв'язку та внесених змін.

Обґрунтоване рішення й порівняння з принаймні однією альтернативою.

Протокол щонайменше двох перевірок: критерій, очікуваний результат, фактичний результат, висновок.

Педагогічне застосування: навчальна вправа або консультаційний матеріал із критеріями перевірки дій користувача.

Аналіз інформаційних та етичних ризиків, доступності й меж перенесення рішення.

Висновки, джерела, декларація використання ІІІ та опис особистого внеску.

Рекомендований обсяг пояснювальної записки — 8–12 сторінок без додатків. До неї додаються конфігурації, код, моделі або інші матеріали відповідно до продукту. За командного виконання кожний учасник подає власні результати й захищає свій внесок.

За 25 балів проєкту оцінюються інтеграція, доопрацювання та придатність цілісного рішення; повторне подання незмінних звітів не є новим результатом. За

15 балів захисту оцінюються особиста демонстрація, аргументація та відповіді. Тривалість представлення — орієнтовно 5–7 хвилин із подальшими запитаннями.

9 Методи навчання та методичне забезпечення

Методи навчання: проблемне пояснення, аналіз освітніх кейсів, практична демонстрація, навчальне проєктування, консультації, взаємне рецензування та рефлексія. Аналіз кейсу підтримує РД1; виконання завдань — РД2; перевірка й обговорення — РД3; інтеграція та захист — РД4.

Матеріальне та програмне забезпечення

Cisco Packet Tracer для підтримуваних функцій; окремий погоджений стенд для решти завдань.

У Cisco Packet Tracer використовуються лише підтримувані функції. Решта дій відпрацьовується на погодженому ізольованому стенді або рівноцінній навчальній моделі. Завдання не є сертифікаційною програмою виробника.

Навчально-методичний комплект: робоча програма, силабус, анотація, матеріали шести тем, вихідний кейс, інструкції до занять, шаблони звітів, завдання модульних перевірок і рубрики. Матеріали та календар доступні через Moodle Академії: <https://moodle.socosvita.kiev.ua>. Посилання на курс і графік консультацій викладач повідомляє перед початком навчання.

10 Контроль і критерії оцінювання

Оцінка накопичується за 100-бальною шкалою. Сам факт відвідування не оцінюється. Окремий екзамен не передбачений.

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

Критерії тематичного продукту

Критерій	Бали	Ознака повного виконання
Виконання вимог	2	Подано всі передбачені елементи завдання.
Коректність рішення	3	Метод і результат відповідають вихідним умовам; немає помилок, які спростовують висновок.

Критерій	Бали	Ознака повного виконання
Перевірка й аргументація	2	Додано докази, пояснено зіставлення результатів і обмеження.
Якість документації	1	Матеріали зрозумілі, відтворювані, з джерелами та належно захищеними даними.

М1 охоплює теми 1–3, М2 — теми 4–6. Кожна перевірка містить шість коротких ситуаційних завдань по 1 балу: правильне рішення з поясненням — 1; частково правильна відповідь — 0,5; неправильна або відсутня — 0. Максимум кожного модуля — 6 балів.

Критерії проєкту та захисту

Об'єкт	Критерій	Бали
Проект	Аналіз проблеми, контексту та вимог	5
Проект	Узгодженість і коректність цілісного рішення	8
Проект	Відтворювані перевірки та аналіз обмежень	5
Проект	Педагогічне застосування і доступність	4
Проект	Етичність, походження матеріалів і документація	3
Разом за проєкт		25
Захист	Демонстрація результату	5
Захист	Обґрунтування рішення та освітнього застосування	5
Захист	Відповіді й особистий внесок	5
Разом за захист		15

Для критеріїв тематичного продукту, проєкту й захисту застосовуються частки їх максимуму: 100 % — повне коректне виконання; 75 % — неістотні недоліки; 50 % — часткове виконання з істотними прогалинами; 25 % — фрагментарний результат; 0 % — результат відсутній або не відповідає завданню. Викладач пояснює виставлені бали.

Підсумкова оцінка

Залік виставляється за сумою накопичених балів: 50–100 — «зараховано», 0–49 — «не зараховано». Невиконаний вид роботи оцінюється в 0 балів. Повторне оцінювання й оскарження здійснюються за локальними процедурами Академії.

Бали	ECTS	Оцінка для заліку
90–100	A	Зараховано

Бали	ECTS	Оцінка для заліку
80–89	B	Зараховано
70–79	C	Зараховано
60–69	D	Зараховано
50–59	E	Зараховано
35–49	FX	Не зараховано; можливість повторного складання
0–34	F	Не зараховано; повторне вивчення дисципліни

11 Орієнтовні контрольні завдання

Приклади ситуаційних завдань

М1. Для завдання «Спроекувати й перевірити сегментацію стенду» виконавець подав лише кінцевий результат без вихідних даних і доказів. Якої інформації бракує для перевірки? Орієнтир: межі об'єкта, джерело даних, метод, критерій, відтворюваний результат.

М2. Під час виконання завдання «Перевірити погоджену конфігурацію та задокументувати обмеження» отримано результат, який суперечить попередньому висновку. Запропонуйте порядок повторної перевірки. Орієнтир: перевірити умови й версії, відтворити дії, зіставити докази, розглянути альтернативне пояснення, уточнити висновок.

Питання для самоконтролю та захисту

1. Які поняття, обмеження та критерії перевірки є визначальними для теми «Вимоги мережевого захисту»? Поясніть їх на матеріалах власного тематичного завдання.

2. Які поняття, обмеження та критерії перевірки є визначальними для теми «Сегментація мережі»? Поясніть їх на матеріалах власного тематичного завдання.

3. Які поняття, обмеження та критерії перевірки є визначальними для теми «Правила контролю доступу»? Поясніть їх на матеріалах власного тематичного завдання.

4. Які поняття, обмеження та критерії перевірки є визначальними для теми «Адміністративне керування»? Поясніть їх на матеріалах власного тематичного завдання.

5. Які поняття, обмеження та критерії перевірки є визначальними для теми «Захист комутації та події»? Поясніть їх на матеріалах власного тематичного завдання.

6. Які поняття, обмеження та критерії перевірки є визначальними для теми «Тренінг безпечної конфігурації»? Поясніть їх на матеріалах власного тематичного завдання.

7. Чим обране рішення відрізняється від альтернативи і чому воно доцільне в заданому освітньому контексті?

8. Які докази дають змогу повторити перевірку, а які лише ілюструють виконання?

9. Які інформаційні, етичні та педагогічні ризики обмежують використання продукту?

10. Як пояснити рішення учасникам професійної освіти й перевірити його засвоєння?

12 Організаційні умови навчання

Доброчесність і авторський внесок

Здобувач зазначає джерела текстів, даних, зображень, конфігурацій і коду; відокремлює власні результати від запозичень. Використання ІІІ декларується із зазначенням засобу, мети, фрагмента роботи та способу перевірки. Відповідальність за достовірність висновків залишається за автором; конфіденційні матеріали до сторонніх сервісів не передаються.

Безпечне виконання завдань

Технічні перевірки здійснюються лише на погодженому навчальному стенді або тестовій копії. Використовуються вигадані чи належно знеособлені дані. Зміни робочих освітніх систем та перевірки сторонніх ресурсів поза навчальним завданням не допускаються. Для соціальних і педагогічних кейсів дотримуються добровільності участі та конфіденційності.

Подання, доступність і зворотний зв'язок

Календар, канал подання, формати файлів і консультації повідомляються до початку курсу. Пропущене завдання відпрацьовується рівноцінним продуктом. Доопрацювання супроводжується журналом змін. За потреби погоджуються доступний формат, асинхронна демонстрація або рівноцінна навчальна модель зі збереженням результатів і критеріїв.

13 Рекомендовані джерела та інформаційні ресурси

Основні джерела

1. Cisco Networking Academy. Cisco Packet Tracer. Офіційні навчальні матеріали з моделювання мереж. <https://www.netacad.com/learning-collections/cisco-packet-tracer>

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. 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>

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>