НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЦИВІЛЬНОГО ЗАХИСТУ

Кафедра цивільного захисту та інформаційних технологій

ЗАТВЕРДЖУЮ
Т.в.о. начальника інституту цивільного
захисту к. держ. управління
Павло РОССОХАТСЬКИЙ

"___" _____ 20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“**Прикладні інформаційні технології, кібербезпека та комп’ютерна підтримка виробничих процесів**”
обов'язкова професійна

за освітньо-професійною програмою “*Охорона праці*”

підготовки *другого (магістерського)* рівня вищої освіти

у галузі знань *J Транспорт та послуги*

за спеціальністю *J4 Охорона праці*

мова навчання *українська*

Схвалено вченою радою
навчально-наукового інституту
цивільного захисту
Протокол від
“___”_____2026 року №____

Черкаси – 2026 рік

Робоча програма навчальної дисципліни “Прикладні інформаційні технології, кібербезпека та комп’ютерна підтримка виробничих процесів” розроблена відповідно до освітньо-професійної програми “Охорона праці” для підготовки здобувачів вищої освіти за другим рівнем вищої освіти в галузі знань J “Транспорт та послуги” зі спеціальності J4 “Охорона праці”

Розробник:
доцент кафедри цивільного захисту та інформаційних технологій, к.т.н., доц., Мурат МАЛЯРОВ.

Робочу програму навчальної дисципліни рекомендовано кафедрою цивільного захисту та інформаційних технологій

Протокол від «___» квітня 2026 року № ___

Начальник кафедри цивільного захисту
та інформаційних технологій
кандидат технічних наук, доцент

Владислав ДЕНДАРЕНКО

«___» квітня 2026 року

Схвалено проектною групою освітньої програми «Охорона праці»

Гарант освітньої програми
доктор наук з державного управління, доцент

Богдан ЦИМБАЛ

«___» _____ 2026 року

1. Мета вивчення навчальної дисципліни

Метою вивчення дисципліни є формування у здобувачів вищої освіти готовності до прийняття ефективних управлінських рішень та керівництва колективами у сфері охорони праці (СК01) шляхом цифровізації процесів безпеки.

Дисципліна спрямована на розвиток навичок критичного пошуку, об'єктивного аналізу та оцінки інформації з використанням спеціальної літературі та баз даних з використанням хмарного інструментарію Google Workspace (GW) для комп'ютерної підтримки виробничих процесів, автоматизації менеджменту безпеки, а також розуміння архітектури кіберфізичних систем підприємства, а також на підготовку здобувачів до оперативного менеджменту та координації команд під час ліквідації техногенних інцидентів та мінімізації цифрових ризиків (кіберзагроз), які можуть становити пряму небезпеку для життя та здоров’я працівників у сучасному комп'ютеризованому виробництві.

У результаті вивчення дисципліни здобувач вищої освіти повинен отримати:

знання:

- методології та алгоритмів прийняття рішень у сфері охорони праці на основі аналізу масивів даних;
- структури, правил ведення та методів моніторингу електронних баз даних, спеціалізованих хмарних реєстрів та різноманітних інформаційних джерел з охорони праці;
- принципів організації та ефективного управління цифровим робочим простором колективу (на базі Google Workspace) для забезпечення безперервності виробничих процесів;
- методів оцінки надійності, валідності та об'єктивності інформації, отриманої з цифрових та літературних джерел, у контексті дослідження виробничих ризиків та кібератак.

уміння/навички:

- здійснювати цілеспрямований пошук інформації у спеціалізованій літературі, міжнародних стандартах (IEC 62443, ISO 45001) та науково-технічних базах даних, критично її аналізувати та об'єктивно оцінювати для розв'язання складних інженерних задач;
- керувати роботою колективу служби охорони праці через розгортання спільних хмарних середовищ, інтерактивних дашбордів та координаційних платформ;
- обґрунтовувати та приймати рішення щодо мінімізації ризиків травматизму на основі прогнозного аналізу інформації, зібраної через хмарні сервіси.

комунікацію:

- здатність чітко, обґрунтовано та оперативно доносити до керівництва, IT-фахівців та членів виробничого колективу управлінські рішення щодо промислової та цифрової безпеки за допомогою інструментів GWfE;
- вміння моделювати та підтримувати ефективні горизонтальні й вертикальні комунікаційні зв'язки всередині колективу в процесі спільної розробки інструкцій, технічних завдань тощо;
- здатність представляти результати об'єктивного аналізу стану ОП підприємства у вигляді інтерактивних звітів та презентувати їх середовищу.

відповідальність та автономію:
- самостійно нести відповідальність за ефективність прийнятих рішень та результатів професійної діяльності колективу в умовах невизначеності або під час ліквідації аварійних ситуацій, спричинених цифровими збоями;
- автономність у прийнятті рішень щодо вибору джерел інформації, методів її верифікації, систематизації та інтеграції в систему управління охороною праці;
- готовність виступати лідером робочих груп із цифрового аудиту безпеки підприємства, демонструючи високий рівень самоорганізації, кібергігієни та професійної відповідальності за збереження життя працівників.

2. Опис навчальної дисципліни

Найменування показників	Форма здобуття освіти	
		заочна (дистанційна)
Статус дисципліни		обов’язкова професійна
Навчальний рік		2 (2026-2027)
Семестр(и)		3
Обсяг дисципліни:		
- в кредитах ЄКТС		3
- загальна кількість годин		90
- кількість модулів		2
Розподіл часу за навчальним планом (в годинах):		
- лекції		4
- практичні заняття		2
- семінарські заняття		-
- лабораторні заняття		-
- курсовий проект (робота)		-

- інші види занять		-
- самостійна робота		84
- індивідуальні практичні завдання за рахунок самостійної підготовки		16
Форма підсумкового контролю		
(курсова робота (курсовий проект); диференційний залік; іспит)		іспит

3. Передумови для вивчення дисципліни

Ефективне засвоєння матеріалу дисципліни базується на міждисциплінарних зв'язках та інтеграції раніше здобутих знань, умінь і практичного досвіду здобувачів вищої освіти.

Перелік раніше вивчених дисциплін:

- «**Теорія систем та системного аналізу**» — забезпечує розуміння методології системного підходу, що є необхідним для аналізу сучасного виробництва як складної кіберфізичної системи та моделювання виробничих ризиків.
- «**Філософія світу та техніки**» — формує світоглядну основу щодо ролі технологічного прогресу, безпекової етики та взаємодії людини й комп’ютера в сучасну епоху.
- «**Іноземна мова в професійній діяльності**» — дозволяє здійснювати ефективний пошук, аналіз та об'єктивну оцінку інформації в англомовній спеціальній літературі, міжнародних базах даних та чинних глобальних стандартах промислової безпеки.

Перелік базових вхідних результати навчання:

- **У сфері ІТ-компетентності**: володіти навичками роботи з персональним комп'ютером, операційними системами та мережею Інтернет на рівні впевненого користувача; мати досвід ефективного використання веб браузерів та пошукових систем.
- **У сфері обробки даних**: володіти базовим інструментарієм роботи з офісними пакетами; вміти створювати, редагувати, форматувати та структурувати текстові документи, а також мати первинні навички управління даними у табличних процесорах.
- **У сфері цифрової культури**: розуміти фундаментальні основи інформаційної безпеки (захист облікових записів, парольна політика), правила безпечної поведінки в мережі та дотримуватися принципів академічної доброчесності й етики використання інформаційних технологій.

4. Результати навчання та компетентності з дисципліни

Відповідно до освітньо-професійної програми “Охорона праці” вивчення обов'язкової навчальної дисципліни повинно забезпечити:

- досягнення здобувачами вищої освіти таких результатів навчання:

Програмні результати навчання	ПРН

Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об’єктивно оцінювати інформацію.	ПРН17

- формування у здобувачів вищої освіти наступних компетентностей:

Програмні компетентності (загальні та професійні)	ЗК, ПК
Здатність приймати ефективні рішення, керувати роботою колективу під час професійної діяльності.	СК01

5. Програма навчальної дисципліни

Теми навчальної дисципліни:

МОДУЛЬ 1. Хмарні технології Google Workspace у зборі, критичному аналізі та об'єктивній оцінці даних безпеки праці

Тема 1.1. Цифрова трансформація менеджменту ОП. Створення внутрішнього інформаційного порталу ОП.

Інформаційний простір «Охорони праці 4.0». Організація спільного документообігу в Google Drive та Документах. Критичний пошук та аналіз нормативно-технічної інформації у базах даних. Побудова спільного хмарного середовища для колективу служби ОП. Керівництво процесом дистанційного навчання та верифікації знань колективу та хмарне управління навчанням у Google Класі

Тема 1.2. Збір та візуалізація виробничих даних та ризиків за допомогою Google Форм та Google Таблиць.

Візуалізація аналітики травматизму за допомогою Google Workspace. Об'єктивна оцінка та графічне представлення інформації через інтерактивні дашборди. Створення цифрових баз даних інспекційного контролю. Формулювання логічних умов та автоматизація розрахунків рівнів небезпеки у хмарі для прийняття рішень.

Модуль 2. Комп'ютерна підтримка виробничих процесів, хмарна кібербезпека.

Тема 2.1. Комп'ютерна підтримка виробництва та оцінка ризиків безпеки праці. Промислова кібергігієна.

Аналіз вразливостей автоматики та прийняття рішень щодо захисту персоналу від аварій, викликаних збоями в ПЗ. Аналіз ризиків людського фактора (фішинг, соціальна інженерія). Стандарти IEC 62443 та ISO 45001. Правила безпечної роботи з комп'ютеризованим обладнанням.

Тема 2.2. Кібербезпека хмарних сервісів та політики безпеки Google.

Керування Спільними дисками Google (Shared Drives) та розмежування доступів. Забезпечення конфіденційності даних. Налаштування політик безпеки, двофакторної автентифікації (2FA) та аудит дій користувачів для запобігання витоку інформації.

Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять (заочна (дистанційна))

Назви модулів і тем	Заочна (дистанційна) форма					
	усього	у тому числі				
		лекції	семінарські заняття	практичні заняття	лабораторні заняття	самостійна робота
3- й семестр						
МОДУЛЬ 1. Хмарні технології Google Workspace у зборі, критичному аналізі та об'єктивній оцінці даних безпеки праці						
Тема 1.1. Цифрова трансформація менеджменту ОП. Створення внутрішнього інформаційного порталу ОП.	20	2				18
Тема 1.2. Збір та візуалізація виробничих даних та ризиків за допомогою Google Форм та Google Таблиць.	22			2		20
Індивідуальне практичне завдання	8					*8*
Разом за модулем 1	*50*	*2*		*2*		*46*
Модуль 2. Комп'ютерна підтримка виробничих процесів, хмарна кібербезпека та антикризове управління колективом						
Тема 2.1. Комп'ютерна підтримка виробництва та оцінка ризиків безпеки праці. Промислова кібергігієна.	16					16
Тема 2.2. Кібербезпека хмарних сервісів та політики безпеки Google.	16	2				14
Індивідуальне практичне завдання	8					*8*
Разом за модулем 2	*40*	*2*				*38*
Підсумковий контроль (іспит)	*Відповідно до Положення про планування та облік навантаження*					
Разом за дисципліну	*90*	*4*		*2*		*84*

Теми лекцій

№ теми	Назва теми лекції	Кількість годин
1.1	1. Хмарні технології Google Workspace у зборі, аналізі та оцінці даних безпеки праці. Візуалізація аналітики за допомогою Google Workspace .	2
2.2	2. Архітектура безпеки хмарного середовища. Політики безпеки, соціальна інженерія та фішинг	2
	Разом	**4**

Теми практичних занять

№ з/п	Назва теми	Кількість годин
1.2	1. Використання Google WorkSpace для експрес-проектування хмарних елементів системи управління охороною праці	2
	Разом	**2**

Індивідуальні завдання:

У межах самостійної роботи з навчальної дисципліни здобувачі вищої освіти виконують комплексні індивідуальні практичні завдання (ІПЗ), які поєднують у собі елементи аналітично-розрахункової діяльності та проектування цифрового середовища:

Індивідуальне практичне завдання за модулем 1. "**Розробка хмарної системи збору даних, моніторингу та візуалізації виробничих ризиків підприємства***".*

Передбачає обробку великих масивів цифрових даних, побудову зведених таблиць, виявлення системних закономірностей виробничого травматизму, а також розробку інтерактивних дашбордів.

Індивідуальне практичне завдання за модулем 2 "**Розгортання захищеної хмарної інфраструктури системи управління ОП на базі Google Сайтів з інтеграцією інструментів зворотного зв'язку***".*

Спрямоване на проектування та розгортання захищеної хмарної інфраструктури: корпоративного Порталу безпеки праці підприємства. Завдання передбачає інтеграцію засобів автоматизованого збору інформації (цифровий зворотний зв'язок) та розробку нормативно-регламентуючих інструкцій з промислової кібербезпеки за допомогою сучасних засобів обчислювальної техніки.

6. Форми та методи навчання і викладання

Вивчення навчальної дисципліни реалізується в таких формах: навчальні заняття за видами, виконання індивідуальних завдань, консультації, контрольні заходи, самостійна робота.

В навчальній дисципліні використовуються такі методи навчання і викладання:

- методи навчання за джерелами набуття знань: словесні методи навчання (лекція, пояснення, бесіда, інструктаж); наочні методи навчання (ілюстрація, демонстрація, спостереження); практичні методи навчання;
- методи навчання за характером логіки пізнання: аналітичний; синтетичний; індуктивний; дедуктивний; традуктивний;
- методи навчання за рівнем самостійної розумової діяльності тих, хто навчається: проблемний виклад; частково-пошуковий;
- інноваційні методи навчання: робота з навчально-методичною літературою та відео метод; навчання з використанням технічних ресурсів; інтерактивні методи; методи організації навчального процесу, що формують соціальні навички;
- самостійна робота.

7. Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є:

- поточний експрес-контроль: оцінюється за результатами проходження 4 тематичних експрес-тестів у хмарному середовищі Google Forms, що дозволяє оперативно перевірити рівень засвоєння лекційного матеріалу під час самостійної роботи;
- захист комплексних індивідуальних практичних завдань (ІПЗ): виконуються у формі презентації аналітичних (проектних) рішень (електронні файлові матеріали, бази даних, аналітичні дашборди та опублікований вебпортал, створених за допомогою сучасних засобів обчислювальної техніки;
- іспит: проводиться під час екзаменаційної сесії у формі виконання підсумкових екзаменаційних тестових (та/або практичних) завдань.

Здобувачі вищої освіти мають можливість отримати додаткові (заохочувальні) бали до семестрового рейтингу за виконання таких видів робіт: ведення структурованого конспекту лекцій, якісне виконання завдань, винесених на самостійне вивчення, аналіз додаткової англомовної спеціалізованої літератури, участь у роботі студентських наукових гуртків та апробація результатів досліджень: підготовка публікацій (тез доповідей, наукових статей) та виступи на науково-практичних конференціях, семінарах, круглих столах з тематики цифровізації безпеки праці та промислової кібергігієни.

8. Критерії оцінювання результатів навчання

Оцінювання рівня навчальних досягнень здобувачів з навчальної дисципліни здійснюється відповідно до Положення про організацію освітнього процесу в Національному університеті цивільного захисту України за 100-бальною шкалою.

Форми поточного та підсумкового контролю

Поточний контроль здійснюється у формі автоматизованого тестового контролю (загалом 4 експрес-контролі, по 2 тести на кожен змістовий модуль). Тестування виконується здобувачами вищої освіти дистанційно в межах самостійної роботи за допомогою цифрових сервісів у чітко визначені календарні терміни.

Модульний підсумковий контроль організовано у формі захисту Індивідуальних практичних завдань (загалом 2 ІПЗ — по одному проекту наприкінці кожного змістового модуля). Метою є комплексна перевірка теоретичної підготовки, рівня сформованості практичних hard skills, навичок автономної дослідницької роботи та готовності до розв'язання складних спеціалізованих задач за фахом. Завдання виконуються під час самостійної роботи за індивідуальними варіантами (або на базі реальних даних власного виробничого підприємства).

Підсумковий контроль проводиться у формі: **іспиту**.

Розподіл балів, які отримують здобувачі, за результатами опанування навчальної дисципліни, формою підсумкового контролю якого є:

іспит:

<table>
<tr><td colspan="5">Розподіл балів заочна (дистанційна) форма</td></tr>
<tr><td colspan="3">Модуль 1</td><td>Іспит</td><td rowspan="6">Сума балів за дисципліну
до 100</td></tr>
<tr><td>Т. 1.1</td><td>Т. 1.2</td><td>Індивідуальне практичне завдання 1</td><td rowspan="5">до 30</td></tr>
<tr><td>до 5</td><td>до 5</td><td>до 25</td></tr>
<tr><td colspan="3">Модуль 2</td></tr>
<tr><td>Т. 2.1</td><td>Т. 2.2</td><td>Індивідуальне практичне завдання 2</td></tr>
<tr><td>до 5</td><td>до 5</td><td>до 25</td></tr>
</table>

Прим. Індивідуальне практичне завдання 1 та 2 є обов'язковою складовою поточного контролю. Здобувачі вищої освіти, які отримали менше ніж 40% від максимальної кількості балів (по кожному індивідуальному практичному завданню) до підсумкового контролю (іспиту) не допускається.

Поточний контроль

Поточний експрес-контроль має на меті оперативну перевірку засвоєння

здобувачами теоретичного матеріалу лекцій та базових положень нормативно-технічних джерел. Кожен із 4 запланованих експрес-тестів оцінюється за 5-бальною шкалою на основі відсотка правильно виконаних завдань. Автоматизована система в фіксує результат, який трансформується у бали за такою шкалою критеріїв:

Відсоток правильних відповідей у тесті	Набраний бал за один ЕК	Якісна характеристика продемонстрованих знань
90% - 100%	5	Відмінно: здобувач володіє теоретичним матеріалом у повному обсязі, бездоганно знає термінологію, архітектуру хмарних сервісів, стандарти кібербезпеки та логіку інженерно-управлінських процесів.
75% - 89%	4	Добре: здобувач добре засвоїв основні теоретичні положення, але припустився незначних помилок у другорядних питаннях або деталях нормативних регламентів.
60% - 74%	3	Задовільно: здобувач володіє мінімально необхідним обсягом знань, орієнтується в базових поняттях курсу, але має прогалини у вивченому матеріалі або фрагментарно розуміє логіку взаємодії ІТ-систем.
35% - 59%	1 - 2	Незадовільно: здобувач демонструє розрізнені, поверхневі знання, плутає ключові терміни, не розуміє базових принципів. Матеріал потребує доопрацювання.
менше 35%	0	Незадовільно (без зарахування): Здобувач не володіє матеріалом, продемонстрував повну відсутність знань або не з'явився на тестування без поважних причин у визначений термін.

Індивідуальні практичні завдання

Кожне ІПЗ оцінюється максимум у 25 балів. Загальна оцінка формується як сума балів за чотирма базовими критеріями, що відображають технічну якість, аналітичну глибину та самостійність виконання роботи.

Розподіл максимальних балів за критеріями

№	Критерій оцінювання	Макс. балів	Що саме оцінюється
1	Технічна коректність та архітектура	8	Правильність налаштування зведених таблиць, формул та графіків (ІПЗ №1) або коректність компонування сайту, форм та прав доступу (ІПЗ №2).
2	Аналітична глибина та обґрунтованість	7	Якість експертного висновку та логіка виявлення ризиків (ІПЗ №1) або повнота та реалістичність розроблених інструкцій з кібергігієни та планів (ІПЗ №2).
3	Оформлення та візуальна культура	5	Зручність використання інструментів, дизайн дашборду чи інтерфейсу сайту, легкість зчитування даних

4	Самостійність та академічна доброчесність	5	Дотримання термінів здачі, унікальність аналізу, здатність здобувача аргументувати свої рішення у коментарях до роботи.
	ЗАГАЛОМ	**25**	**Максимальна оцінка за одне ІПЗ.**

Шкала якісної оцінки проекту.

Залежно від рівня виконання, сумарний бал за ІПЗ виставляється за такою градацією:

23 - 25 балів: Робота виконана бездоганно, всі формули, зведені таблиці чи хмарні права доступу налаштовані правильно. здобувач продемонстрував глибокий аналіз даних або створив висококласні нормативні інструкції, які можна прямо зараз впроваджувати на реальному виробництві. Проект має високу візуальну культуру (інтерактивний, зручний у навігації). Дотримано всіх термінів.

19 - 22 балів: Завдання виконано в повному обсязі, хмарні сервіси працюють коректно. Аналітичний звіт або розроблені інструкції є правильними, але мають загальний характер, недостатньо враховують унікальну специфіку конкретного підприємства. Припущено 1-2 незначні помилки в інтерфейсі сайту чи дизайні графіків, які не впливають на загальне сприйняття даних.

15 - 18 балів: Робота виконана, але є збої у розрахунках, не налаштоване умовне форматування або порушена логіка розмежування прав доступу на Диску. Аналіз даних поверхневий («констатація фактів» замість пошуку причин), а інструкції з кібербезпеки скопійовані з типових шаблонів без інженерного опрацювання. Візуальне подання хаотичне, навігація сайтом або дашбордом ускладнена.

9 - 14 балів: Завдання виконано частково (менше 60% від вимог). Ключові елементи (зведені таблиці, форми або сам сайт) відсутні або повністю непрацездатні. Управлінські висновки відсутні. Робота повертається на обов'язкове доопрацювання з пониженням максимального підсумкового балу.

0 балів : Роботу не надано у визначені терміни без поважних причин, або виявлено 100% плагіат (копіювання варіанта інших здобувачів).

Підсумковий контроль.

Загальний бал за іспит (30 балів) складається з двох частин: Практичної (до **20 балів**) та Теоретичної складової (до **10 балів**).

Практична складова (20 балів) може реалізуватися в одному з двох альтернативних форматів:

ВАРІАНТ А: Комплексний публічний захист наскрізного проекту

Здобувач виступає в ролі керівника служби охорони праці та презентує раніше розроблений інтегрований Портал безпеки підприємства (на базі Google Сайтів та хмарних регламентів).

18 - 20 балів: Здобувач вільно володіє матеріалом, демонструє відмінні презентаційні навички. Професійно, аргудовано та вичерпно відповідає на всі

додаткові запитання викладача (моделювання виробничих ситуацій та кібератак).

14 - 17 балів: Проект презентовано впевнено, хмарна інфраструктура працює без збоїв. Здобувач розуміє логіку побудованого Порталу, але під час відповідей на додаткові запитання йому бракує управлінської впевненості.

11 - 13 балів: Захист має характер простого переліку виконаних технічних дій («я створив таблицю, я вставив графік»). Здобувач відчуває труднощі при спробі обґрунтувати свої рішення з точки зору менеджменту.

0 - 10 балів: Здобувач не може пояснити логіку функціонування власного сайту чи аналітичного дашборду. Демонструє неспроможність приймати рішення у змодельованих ситуаціях.

ВАРІАНТ Б: Виконання експрес-практичних вправ та надання управлінських рекомендацій на іспиті

Безпосередньо під час іспиту здобувач отримує індивідуальну експрес-задачу: аналіз оперативного цифрового масиву інцидентів (вправи на обчислювальну техніку в Google Sheets) та написання термінових рекомендацій (антикризового плану) для керівництва підприємства.

18 - 20 балів: Експрес-вправи виконані технічно бездоганно і в повному обсязі. Здобувач сформулював глибокі, логічні та нормативно обгрунтовані рекомендації щодо ліквідації наслідків цифрового чи виробничого інциденту, продемонструвавши високий рівень антикризового менеджменту.

14 - 17 балів: Практичні вправи виконані правильно, але в аналітичній записці з рекомендаціями допущено незначні неточності, або запропоновані заходи мають дещо загальний, шаблонний характер.

11 - 13 балів: Технічні вправи виконані частково (допущені помилки у формулах чи логічних зв'язках). Надані рекомендації поверхневі, не містять чіткого покрокового алгоритму дій для колективу.

0 - 10 балів: Здобувач не впорався з практичними вправами на обчислювальній техніці, аналітичні висновки та рекомендації відсутні або повністю не відповідають вимогам промислової безпеки.

Теоретична складова (10 балів)

Виконання підсумкового екзаменаційного комп'ютерного тесту або відповідь на питання білета щодо міжнародних нормативів (IEC 62443, ISO 45001) та архітектури промислових систем.

9 - 10 балів: Глибоке знання теоретичної бази (від 90% до 100% правильних відповідей), повне розуміння архітектур безпеки кіберфізичних систем.

7 - 8 балів: Повні знання теорії (74%-89% відповідей), але присутні поодинокі неточності у формулюваннях стандартів.

6 балів: Знання базових понять є (60%-73% відповідей), але відповіді фрагментарні, здобувачі важко пояснити взаємозв'язок між загрозами.

0 - 5 балів: Незадовільний рівень володіння теоретичним матеріалом курсу (менше 60% правильних відповідей).

9. Засоби провадження освітньої діяльності

Провадження освітньої діяльності з дисципліни здійснюється шляхом використання:

1. Аудиторних форм навчання - лекції, практичні та лабораторні заняття з використанням мультимедійних засобів, інтерактивних презентацій, демонстраційних прикладів програмного забезпечення.
2. Самостійної роботи здобувачів освіти - опрацювання теоретичного матеріалу, виконання індивідуальних завдань, підготовка звітів та презентацій.
3. Інформаційно-комунікаційних технологій - використання хмарних сервісів (Google Workspace), систем управління електронним навчанням (Google Classroom) та сервісу електронних комунікацій (Google Meet).
4. Навчально-методичного забезпечення - підручників, навчальних і методичних посібників, відеоматеріалів та електронних ресурсів у сфері охорони праці.
5. Технічних засобів навчання - персональних комп’ютерів, мультимедійних комплексів, проєкторів, локальних мереж та засобів доступу до мережі Інтернет.

10. Політика викладання навчальної дисципліни

Взаємодія між викладачем та здобувачами базується на принципах професійної етики, партнерства, взаємоповаги та обов'язкового використання цифрових технологій.

Політика щодо дедлайнів та перескладання.

- Індивідуальні практичні завдання (ІПЗ №1 та ІПЗ №2), а також тести експрес-контролю мають бути виконані та надані на перевірку у терміни, визначені графіком самостійної роботи (за 3 тижні до початку екзаменаційної сесії).
- Роботи, надані з порушенням дедлайну без поважних причин, можуть бути оцінені з пониженням максимального балу на 20%.
- Здобувачі, які набрали за тест або ІПЗ незадовільний бал (менше 60% від максимуму), мають право на одну спробу покращення результату до початку іспиту.

Політика цифрової взаємодії та комунікації.

- Усі навчальні матеріали, варіанти завдань, посилання на тести Google Forms та критерії оцінювання розміщуються у спільному хмарному просторі курсу на платформі Google Class.
- Результати ІПЗ приймаються виключно у вигляді цифрових посилань на відповідні хмарні ресурси (робочі таблиці, дашборди, опублікований Google Сайт). Доступи до ресурсів мають бути відкриті для викладача.
- Консультації та обговорення організаційних питань відбуваються у визначені часи через офіційні канали зв'язку (корпоративна пошта, системи електронних комунікацій Google Meet та Google Chat).

Політика академічної доброчесності.

- Очікується, що індивідуальні завдання виконуються здобувачам самостійно на базі його варіанта або реальних даних його підприємства.
- Виявлення 100% копіювання розрахунків, аналітичних звітів чи інструкцій в інших здобувачів є підставою для анулювання результату роботи без права на легке перескладання.
- Допускається використання генеративних моделей (на кшталт ChatGPT або Gemini) як допоміжного інструменту для пошуку ідей чи структурування тексту регламентів. Проте, фінальний аналіз даних, логіка зведених таблиць та управлінські рекомендації мають бути особистим інтелектуальним продуктом здобувача. Відповідальність за технічну та нормативну точність згенерованого тексту повністю несе здобувач.

11. Рекомендовані джерела інформації

Література

1. Освітньо-професійна програма «Охорона праці» за спеціальністю J4 “Охорона праці” у галузі знань J “Транспорт та послуги”. - Режим доступу: https://nuczu.edu.ua/images/topmenu/osvitnya_diyalnisti/osvitni_programi/2025/m/J4_.pdf (дата звернення: 30.04.2026).

2. Маляров М., Зажома В., Дендаренко В. Основи інформаційних технологій : навчальний посібник. Черкаси: НУЦЗ України, 2025. - 194 с. URL: https://elibrary.net.ua/3132/ (дата звернення: 30.04.2026).

3. Маляров М., Говаленков С., Гончар С., Шевченко Р. Інноваційні технології: форми та методи здійснення освітньої діяльності в закладах вищої освіти : курс лекцій. Черкаси : НУЦЗУ, 2025. 87 с. URL: https://elibrary.net.ua/2778/ (дата звернення: 30.04.2026).

4. Маляров М., Гоменюк О., Зажома В., Дендаренко В. LibreOffice Calc. Від основ до автоматизації : навчально-методичний посібник [відеокурс]. Черкаси : НУЦЗ України, 2026. URL: https://elibrary.net.ua/3133/ (дата звернення: 30.04.2026).

5. Маляров М. В., Христич В. В., Гусева Л. В., Паніна О. О. Обробка інформації за допомогою пакету LibreOffice: практикум. Частина 1. LibreOffice Calc. Харків: НУЦЗУ, 2021. 116 с. URL: http://repositsc. nuczu.edu.ua/handle/123456789/ 13120 (дата звернення: 04.05.2026).

6. Бородкіна І. Л., Бородкін Г. О. Web-технології та Web-дизайн: застосування мови HTML для створення електронних ресурсів : навчальний посібник. Київ : Ліра-К, 2020. 212 с. ISBN 978-617-7844-14-2.

7. Буйницька О. П. Інформаційні технології та технічні засоби навчання : навчальний посібник. Київ : Центр учбової літератури, 2018. 240 с. ISBN 978-611-01-0996-3.

8. Маляров М. В., Христич В. В. Використання нейронних мереж для

обробки результатів моніторингу НС на природних територіях // Запобігання надзвичайним ситуаціям і їх ліквідація : матеріали науково-практичного семінару (Харків, 21 лютого 2019 р.). Харків : НУЦЗ України, 2019. С. 111-113.

9. Христич В. В., Маляров М. В. Використання хмарних технологій для автоматизації обліку успішності здобувачів освіти // Молодь у світі сучасних технологій : матеріали міжнародної науково-практичної конференції (Херсон, 4-5 червня 2020 р.). Херсон, 2020. С. 401-404.

10. ДСТУ IEC 62443-2-1:2022 (IEC 62443-2-1:2010, IDT). Промислові комунікаційні мережі. Кібербезпека мереж і систем. Частина 2-1. Побудова програми кібербезпеки для систем промислової автоматизації та контролю : Національний стандарт України. — [Чинний від 2023-01-01]. — Київ : ДП «УкрНДНЦ», 2022. — 74 с. — (Кібербезпека промислових систем).

11. ДСТУ ISO 45001:2019 (ISO 45001:2018, IDT). Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування : Національний стандарт України. — [Взамен ДСТУ-П OHSAS 18001:2010 ; чинний від 2021-01-01]. — Київ : ДП «УкрНДНЦ», 2019. — 46 с. — (Системи менеджменту).

12. Ткаченко В. А., Касілов О. В., Рябик В. А. Комп'ютерні мережі та телекомунікації : навчальний посібник. Харків : НТУ «ХПІ», 2011. 224 с.

Інформаційні ресурси

1. Google Workspace Learning Center (Офіційні інструкції з налаштування Google Таблиць та зведених таблиць) — URL: https://support.google.com/a/users/answer/9282959
2. Looker Studio Help Center (Документація та посібники з побудови інтерактивних аналітичних дашбордів) — URL: https://support.google.com/looker-studio/
3. Google Sites Офіційне керівництво (Покрокові інструкції з архітектури та публікації вебсайтів) — URL: https://support.google.com/sites/

Розробник:
Доцент кафедри
канд. техн. наук, доцент

Мурат МАЛЯРОВ