СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«СУЧАСНІ МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Савченко Віталій Анатолійович, доктор технічних наук, професор,
професор кафедри Управління кібербезпекою та захистом інформації</td><td>Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: v.savchenko@duikt.edu.ua
сторінка курсу в Classroom -
https://classroom.google.com/c/NzA4MzAxMjU4MzU5?cjc=73zt3bp
код доступу - 73zt3bp</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="2">доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">125 Кібербезпека та захист інформації</td><td>Семестр</td><td colspan="2">1, 2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Кібербезпека</td><td>Тип дисципліни</td><td colspan="2">Цикл обов’язкових компонент ОНП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>4</td><td>120</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
36</td><td>Лабораторних занять
-</td><td>Самостійна підготовка
66</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="5">Методологія наукових досліджень у кібербезпеці.
Теоретичні та практичні проблеми технічного захисту інформації.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="5">Науково-педагогічна практика.</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">Формування у здобувачів освіти базових теоретичних знань, умінь і практичних навичок, необхідних для застосовування сучасних способів, методів та засобів управління кібербезпекою та захистом інформації.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="3">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Фахові компетентності (СК)</td></tr>
<tr><td colspan="3"></td><td colspan="5">ФК-1. Інтегративна компетентність – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо.
ФК-2. Соціально-психологічна компетентність (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо.
ФК-6. Політехнічна компетентність – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування</td></tr>
</table>

	різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ФК-7. Інженерна компетентність** – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо. **ФК-8. Ділова компетентність** – здатність і готовність здійснювати ефективну професійну діяльність у відповідній галузі, надавати інфокомунікаційні послуги та послуги безпеки; здатність до планування й реалізації заходів із захисту інформації в ІКС, створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.
Програмні результати навчання (ПРН)	
ПРН-12. Уміти визначати основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій, практично-семінарських занять). **ПРН-15**. Уміти орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки. **ПРН-16**. Уміти розробляти та проектувати нові, вдосконалювати існуючі системи управління інформаційною безпекою. **ПРН-21**. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. **ПРН-25**. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності. **ПРН-28**. Бути здатним до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ПРН-29**. Уміти розробляти та впроваджувати раціональні технології інформаційної безпеки, програми і методики випробувань систем інформаційної та кібербезпеки **ПРН-30**. Бути здатним до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1. Основи теорії управління складними процесами та системами			
Тема 1. Основні положення теорії управління у сфері інформаційної безпеки **Знати:** Стан розвитку теорії систем та її елементи. Нормативну базу розробки та впровадження систем управління інформаційною безпекою. Місце і роль управління в системі забезпечення інформаційної безпеки організації. Критерії і методологію оцінки безпеки інформаційних технологій. **Вміти:** Ставити завдання на виконання практичної задачі з побудови функціональних структур підприємств. Аналізувати ризики в підприємницькій діяльності. Оцінювати ефективність управління організацією. Оцінювати управління економічною та інформаційною безпекою підприємства. Здійснювати системний аналіз інформаційних систем.			

Формування компетентностей: ФК-1, ФК-2, ФК-8. **Результати навчання:** ПРН-12, ПРН-16, ПРН-28. **Рекомендовані джерела:** 1-7, 9-10, 12, 25-29.			
Стан розвитку теорії систем та її елементи	Лекція 1 2 год		Лекція-візуалізація
Нормативна база розробки та впровадження систем управління інформаційною безпекою	Лекція 2 2 год		Лекція-візуалізація, експрес-опитування здобувачів
Місце і роль управління в системі забезпечення інформаційної безпеки організації	Лекція 3 2 год		Лекція-візуалізація, експрес-опитування здобувачів
Критерії і методологія оцінки безпеки інформаційних технологій	Практичне заняття 1 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Завдання на виконання практичної задачі з побудови функціональних структур підприємств	Практичне заняття 2 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Аналіз ризику в підприємницькій діяльності	Практичне заняття 3 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Оцінка ефективності управління організацією	Практичне заняття 4 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Оцінка управління економічною та інформаційною безпекою підприємства- на прикладі.	Практичне заняття 5 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Системний аналіз інформаційних систем.	Практичне заняття 6 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 1. Основні положення теорії управління у сфері інформаційної безпеки	Самостійна робота 22 год	8 балів	1. Визначення управління та його основні процеси. 2. Сутність методів управління. 3. Класифікація систем управління. 4. Нормативна база розробки та впровадження систем управління інформаційною безпекою. 5. Єдині критерії оцінки безпеки інформаційних технологій. 6. Загальна методологія оцінки безпеки інформаційних технологій. 7. Система управління організації як об'єкт дослідження. 8. Інформація як продукт захисту в інформаційній системі. 9. Підходи до побудови системи забезпечення інформаційної безпеки.

			10. Методика побудови функціональної структури підприємств з підрозділами забезпечення інформаційної безпеки. 11. Методики оцінки небезпек і управління ризиком в підприємницькій діяльності. 12. Оцінка ефективності управління організацією 13. Оцінка управління економічною та інформаційною безпекою підприємства.
Тема 2. Методологічні підходи до дослідження систем управління інформаційною безпекою **Знати:** Методи досліджень системи управління інформаційною безпекою. Методи менеджменту безпеки інформаційних технологій. Методичні підходи до виявлення, прогнозування і оцінювання загроз та інформаційних ризиків функціонуванню підприємства. Аналіз та синтез як методи дослідження і проектування організацій. Концепція та основні напрями забезпечення інформаційної безпеки. Кращі практики створення політик безпеки. Загрози безпеці систем і способи їх реалізації. **Вміти:** Застосовувати метрики управління інформаційною безпекою. Застосовувати: методи виявлення загроз функціонуванню підприємства; методи прогнозування загроз функціонуванню підприємства; методи оцінювання загроз та інформаційних ризиків. **Формування компетентностей:** ФК-6, ФК-7. **Результати навчання:** ПРН-15, ПРН-21, ПРН-25. **Рекомендовані джерела:** 8,12,22,29			
Методи досліджень системи управління інформаційною безпекою	Лекція 4 2 год		Лекція-візуалізація
Методи менеджменту безпеки інформаційних технологій	Лекція 5		Лекція-візуалізація, експрес-опитування здобувачів
Методичні підходи до виявлення, прогнозування і оцінювання загроз та інформаційних ризиків функціонуванню підприємства	Лекція 6 2 год		Лекція-візуалізація, експрес-опитування здобувачів
Аналіз та синтез як методи дослідження і проектування організацій	Практичне заняття 7 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Концепція та основні напрями забезпечення інформаційної безпеки	Практичне заняття 8 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Кращі практики створення політик безпеки	Практичне заняття 9 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Загрози безпеці систем і способи їх реалізації	Практичне заняття 10 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Використання метрик управління інформаційною безпекою	Практичне заняття 11 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Проміжний контроль. Виконання кваліфікаційних завдань. Тестування	Практичне заняття 12	2 бали	Виконання завдань на практичне застосування знань і вмінь.

	2 год		
Тема 2. Методологічні підходи до дослідження систем управління інформаційною безпекою.	Самостійна робота 22 год	8 балів	1. Аналіз та синтез як методи дослідження і проектування організацій 2. Закон єдності аналізу і синтезу. 3. Цілі, завдання аналізу і синтезу систем управління. 4. Кращі практики створення політик безпеки від компаній IBM, Cisco Systems, Microsoft, Symantec і SANS. 5. Концепція та основні напрями забезпечення інформаційної безпеки. 6. Методи виявлення загроз функціонуванню підприємства. 7. Методи прогнозування загроз функціонуванню підприємства. 8. Методи оцінювання загроз та інформаційних ризиків. 9. Можливості моделей загроз безпеці систем і способів їх реалізації. 10. Підходи до визначення критеріїв уразливості і стійкості систем деструктивним впливам. 11. Вимірювання інформаційної безпеки. 12. Процес визначення метрик і їх оцінки відповідно до нормативних документів
Розділ 2. Застосування сучасних методів дослідження у сфері управління інформаційною та кібербезпекою			
Тема 3. Методологічні підходи до побудови систем управління інформаційною безпекою **Знати: Методи м**оделювання процесів в системах управління інформаційною безпекою. Концептуальні підходи до побудови ефективної системи інформаційної безпеки. Технології управління безперервністю бізнесу на основі управління інформаційними інцидентами. **Вміти:** Застосовувати процесний та комбінований підходи до створення СУІБ організації. Застосовувати методи аналізу подій інформаційної та кібербезпеки. Здійснювати моніторинг інформаційної безпеки. **Формування компетентностей:** ФК-7, ФК-8. **Результати навчання:** ПРН-28, ПРН-29, ПРН-30. **Рекомендовані джерела:** 5,7,9-14,24-29			
Моделювання процесів в системах управління інформаційною безпекою	Лекція 7 2 год		Лекція-візуалізація
Концептуальний підхід до побудови ефективної системи інформаційної безпеки	Лекція 8 2 год		Лекція-візуалізація, експрес-опитування здобувачів
Управління безперервністю бізнесу на основі управління інформаційними інцидентами	Лекція 9 2 год		Лекція-візуалізація, експрес-опитування здобувачів
Застосування процесного підходу до створення СУІБ організації	Практичне заняття 13 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Застосування комбінованого підходу до створення СУІБ організації	Практичне заняття 14	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.

	2 год		
Практика проходження перевірки СУІБ на відповідність вимогам стандартів ISO	Практичне заняття 15 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Застосування методу аналізу ієрархій в системному аналізі	Практичне заняття 16 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Практика моніторингу подій інформаційної безпеки	Практичне заняття 17 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 3. Методологічні підходи до побудови систем управління інформаційною безпекою	Самостійна робота 22 год	10 балів	1. Концептуальний підхід до побудови ефективної системи інформаційної безпеки 2. Підхід та методика до побудови ефективної системи ІБ 3. Заходи щодо захисту інформації. 4. Процесний підхід та методика управління організацією. 5. Використання вимог із стандартизації до систем процесів управління інформаційною безпекою. 6. Впровадження системи управління інформаційною безпекою. 7. Нормативні вимоги до СУІБ з управління ризиками ІБ (відповідно до стандартів ISO / IEC 2700-к) 8. Комбінований підхід в процесах управління інформаційною безпекою. 9. Застосування підходу до створення СУІБ організації 10. Розробка та впровадження системи управління інцидентами інформаційної безпеки. 11. Методика управління інцидентами інформаційної безпеки 12. Забезпечення готовності організації до інцидентів інформаційної безпеки і безперервності діяльності бізнесу. 13. Концепція готовності до інцидентів інформаційної безпеки і безперервності діяльності. 14. Програма забезпечення готовності до інцидентів інформаційної безпеки і безперервності діяльності. 15. Вимоги до планування безперервності бізнесу. 16. Застосування методу аналізу ієрархій в системному аналізі інформаційної безпеки. 17. Особливості застосування методу аналізу ієрархій . 18. Метод аналізу ієрархій у вирішенні задач. 19. Практика моніторингу подій та реагування на події інформаційної безпеки.

			20. Основні структури SIEM-систем з моніторингу подій інформаційної безпеки. 21. Підхід і методика оцінки ефективності процесу управління подіями інформаційної безпеки.
Іспит	Практичне заняття 18 2 год	40 балів	Іспит у письмовій формі.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп‘ютерне обладнання, мережа Інтернет;
- Комп’ютерний клас для проведення занять: Security Operation Center.
- Програмне забезпечення перевірки СУІБ.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Савченко В.А. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. / Ю. М. Якименко, В. А. Савченко, С. В. Легомінова. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf.
2. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. https://duikt.edu.ua/uploads/l_1426_56444238.pdf
3. Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ : ТОВ «ТРОПЕА», 2024. 104 с. https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/scientific-publications/monographs/information_security_and_hybrid_threats.pdf .
4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf?srsltid=AfmBOooKlUg0smK991mL4FTTxgPDdWByvtE2XFVfGhLKscRn-MwCT7vt
5. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства: монографія. Вінниця: Європейська наукова платформа, 2020. 342 с. URL: https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859.
6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.
7. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.
8. Якименко Ю. М., Чернявський І. Р. Ризикоорієнтований підхід до управління інформаційною безпекою на підприємстві. *Сучасний захист інформації*. 2022. № 2(50). С. 38-45. URL: http://journals.dut.edu.ua/index.php/dataprotect/issue/view/164.
9. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. http://web.kpi.kharkov.ua/cep/wp-content/uploads/sites/217/2024/01/Upravlinnya-informatsijnoyu-bezpekoyu.pdf
10. П.Г. Сидоркін, С.О. Горліченко, В.С. Некоз, М.В. Шилан. «Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 FOR RISK». - 2023. https://duikt.edu.ua/uploads/l_2234_89731024.pdf
11. Карпович І.М., Гладка О.М., Калашніков В.І.. «Моделювання процесів аналізу ризиків інформаційної безпеки як спосіб оптимізації витрат». - 2022. https://duikt.edu.ua/uploads/l_2163_29474377.pdf
12. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*: матеріали II Міжнародна наук.-практ. конф. (м. Київ, Україна, 11 лютого 2021 р.). Київ: ДУТ, 2021. С. 279-282. URL: http://www.dut.edu.ua/uploads/n_9074_59003267.pdf.
13. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2024. – 370 с

https://profbook.com.ua/index.php?route=product/product/download&product_id=8999&download_id=2047&srsltid=AfmBOopCqtAUcJn81p9V9Tj06MA3Vurf20gX2tJlIve2JhrpPRUdc8Ul
14. Якименко Ю. М. Методичні підходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави:* збірник тез наукових доповідей XII матеріали Всеукр. наук.-практ. конф. (м. Київ, Україна, 26 березня 2021р.). Київ: Нац. акад. СБУ, 2021. С. 162-164. URL: https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf.
15. Якименко Ю. М. Використання спеціалізованих платформ і рішень з безпеки інформації в системному аналізі інформаційної безпеки організацій. *Цифрова трансформація кібербезпеки*: матеріали Всеукр. наук.-практ. конф., (м. Київ, Україна, 25 березня 2021 р.). Київ: ДУТ, 2021. С. 5-8. URL: http://www.dut.edu.ua/uploads/n_9126_17047934.pdf
16. Мужанова Т. М., Легомінова С. В., Якименко Ю. М., Мордас І. В. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. *Кібербезпека: освіта, наука, техніка.* № 1(13). С. 50-62. URL: https://doi.org/10.28925/2663-4023.2021.13.5062.
17. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. *Кібербезпека: освіта, наука, техніка.* 2021. № 4(12). С. 36-50. URL: https://doi.org/10.28925/2663-4023.2021.12.3650.
18. Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків. *Актуальні проблеми кібербезпеки:* матеріали Всеукр. наук. конф., (м. Київ, Україна, 27 жовтня 2021 р.). Київ: ДУТ, 2021. С.173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.
19. Якименко Ю. М. Вирішення проблеми забезпечення безперервності бізнесу завдяки впровадженню центру кіберстійкості *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:* матеріали II Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 24 лютого 2022 р.). Київ: ДУТ, 2022. С. 15-18. URL: https://dut.edu.ua/uploads/p_2121_33783557.pdf.
20. Якименко Ю. М., Дьячук О. С. Методичний підхід до забезпчення безперервності бізнесу й відновлення після інциденту. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали III Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 23 лютого 2023 р.). Київ: ДУТ, 2023. С. 49-52.
21. Якименко Ю. М., Рабчун Д. І., Капелюшна Т. В. Використання методичних підходів з системного аналізу до захисту об'єктів критичної інфраструктури. *Виклики і загрози для критичної інфраструктури*: матеріали Міжнародн. наук.-практ. конф. (м. Київ, Україна, 21-22 березня 2023 р.). Київ: ДУТ, 2023. 5с.
22. Якименко Ю. М., Рабчун Д. І., Мужанова Т. М., Запорожченко М. М. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємств. *Кібербезпека: освіта, наука, техніка:* електронне фахове наукове видання. Київ, 2023. С.18.
23. Підвищення ролі DLP - систем у розслідуванні інцидентів (кіберінцидентів) інформаційної безпеки. *Цифрова трансформація кібербезпеки*: матеріали Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 27 квітня 2023 р.). Київ: ДУТ, 2023.
24. О.В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». - 2021. https://duikt.edu.ua/uploads/l_1066_72351971.pdf
25. А.М. Гребенюк, Л.В. Рибальченко. «Основи управління інформаційною безпекою». - 2020. https://duikt.edu.ua/uploads/l_486_55027317.pdf
26. Легомінова С. В., Мужанова Т. М., Якименко Ю. М., Власенко В. О. Засоби інформування й навчання персоналу у сфері інформаційної безпеки в умовах цифровізації. Зв'язок. 2021. №4 (152). С.14-16. URL: http://con.dut.edu.ua/index.php/communication/article/view/2543.
27. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, V. Savchenko and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
28. Савченко, В. А. (2023). Сучасні виклики та загрози цифровій трансформації компаній. Сучасний захист інформації, 1(53), 6–11. https://doi.org/10.31673/2409-7292.2023.010001.
29. Савченко, В. А. (2024). Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації. Зв'язок, 3(169). 12-17. https://doi.org/10.31673/2412-9070.2024.031217

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і семінарських занять, а також самостійну роботу.

- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 60 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	34 бали
	• Самостійна робота	26 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	40 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції.	3 бали
- Стаття у фаховому виданні.	5 балів
- Стаття в іноземному рецензованому виданні.	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка /***запис в екзаменаційній відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних/контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)

82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни.	Добре / Зараховано (B)
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які	Незадовільно з обов'язковим повторним

		окреслює мета та завдання дисципліни.	вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.