СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Сучасні методи управління інформаційною безпекою»

Лектор курсу			**Савченко Віталій Анатолійович,** доктор технічних наук, професор, директор Навчально-наукового інституту захисту інформації; **Якименко Юрій Михайлович**, кандидат військових наук, доцент, доцент кафедри "Управління інформаційною та кібернетичною безпекою"		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**yakum14@ukr.net; **сторінка курсу в Moodle –**	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	доктор філософії	
Спеціальність			125 Кібербезпека		**Семестр**	2	
Освітня програма			КІБЕРБЕЗПЕКА		**Тип дисципліни**	основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18	-	36	-	66

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у аспірантів базових теоретичних знань, умінь і практичних навичок, необхідних для застосовування сучасних способів, методів та засобів щодо управління інформаційною безпекою.

Компетентності відповідно до освітньої програми

Загальні компетентності (ЗК)	**Фахові компетентності (ФК)**
	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… сучасними інформаційними та безпековими технологіями; здатність до застосування 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). **ПРН15** Уміти орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки. (ІБ). **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**
ЗМІСТОВИЙ МОДУЛЬ **1 «ВИМОГИ З ТЕОРІЇ УПРАВЛІННЯ СКЛАДНИМИ ПРОЦЕСАМИ ТА СИСТЕМАМИ»**			

Тема 1. ***Основні положення теорії управління у сфері інформаційної безпеки*** ***Знати***: основні терміни і визначення з теорії управління і управління інформаційною безпекою (ІБ), їх основні процеси, сутність методів управління, класифікацію систем управління, вимоги міжнародних документів в галузі інформаційної безпеки і стан впровадження міжнародних стандартів в Україні, місце і роль управління в системі забезпечення інформаційної безпеки організації. ***Вміти:*** використовувати методологію оцінки безпеки інформаційних технологій; будувати функціональні структури підприємств з підрозділами забезпечення інформаційної безпеки, проводити аналіз ризику в підприємницькій діяльності відповідно до методики управління ризиком, оцінювати ефективність управління організацією відповідно до методики оцінки ефективності управлінських рішень, оцінювати управління економічною та інформаційною безпекою підприємства. ***Формування компетенцій:*** ФК-1, ФК-2, ФК-6 ***Результати навчання:*** ПРН21, ПРН-25**,**ПРН28, ПРН30 ***Рекомендовані джерела:*** 1-10,12,14-16,18,31-34,36-42	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування аспірантів
	Лекція 3		Лекція-візуалізація, експрес-опитування аспірантів
	Практичне заняття 1		Використання критеріїв і методології оцінки безпеки інформаційних технологій - на прикладах. Обговорення результатів
	Практичне заняття 2		Виконання практичної задачі з побудови функціональних структур підприємств. Обговорення результатів
	Практичне заняття 3		Аналіз ризику в підприємницькій діяльності - на прикладі. Обговорення результатів
	Практичне заняття 4		Оцінки ефективності управлінських рішень. Обговорення результатів
	Практичне заняття 5		Оцінка управління економічною та інформаційною безпекою підприємства- на прикладі. Обговорення результатів
	Практичне заняття 6		Системний аналіз інформаційних систем.
Тема 2***. Методологічні підходи до дослідження систем управління інформаційною безпекою*** ***Знати***: основні методи дослідження і проектування організацій та їх систем управління, концепцію та основні напрями забезпечення інформаційної безпеки організації, кращі практики створення політик безпеки (ПБ); методичні підходи до виявлення, прогнозування і оцінювання загроз та інформаційних ризиків функціонуванню підприємства ***Вміти***: створювати політики безпеки ІБ з використанням підходів до розробки кращих практик ПБ від компаній IBM, Cisco Systems, Microsoft, Symantec і SANS, Використовувати підходи до визначення критеріїв уразливості і стійкості систем деструктивним впливам, оцінювати ефективність інформаційної безпеки організації за допомогою метрик безпеки.	Лекція 4	5,5*	Лекція-візуалізація
	Лекція 5		Лекція-візуалізація, експрес-опитування аспірантів
	Лекція 6		Лекція-візуалізація, експрес-опитування аспірантів
	Практичне заняття 7		Аналіз та синтез систем управління. Обговорення результатів
	Практичне заняття 8		Відпрацювання методики комплексного підходу до забезпечення безпеки організації. Обговорення результатів
	Практичне заняття 9		Аналіз кращіх практик ПБ від компаній IBM, Cisco Systems, Microsoft, Symantec і SANS. Обговорення результатів
	Практичне заняття 10		Аналіз можливості моделей загроз безпеці систем і способів їх реалізації. Обговорення результатів
	Практичне заняття 11		Використання метрик безпеки в управлінні інформаційною безпекою. Обговорення результатів

Формування компетенцій: ФК-6, ФК-7 ***Результати навчання:*** ПРН16,ПРН21, ПРН28, ПРН30 ***Рекомендовані джерела:*** 11-12,18,28,35,36,40	Практичне заняття 12		Модульний контроль №1. Виконання кваліфікаційних завдань. Тестування
Тема 1. Основні положення теорії управління у сфері інформаційної безпеки **Тема 2.** Методологічні підходи до дослідження систем управління інформаційною безпекою	Самостійна робота		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. 14. Аналіз та синтез як методи дослідження і проектування організацій 15. Закон єдності аналізу і синтезу. 16. Цілі, завдання аналізу і синтезу систем управління. 17. Кращі практики створення політик безпеки від компаній IBM, Cisco Systems, Microsoft, Symantec і SANS 18. Концепція та основні напрями забезпечення інформаційної безпеки. 19. Оцінка можливостей програми ГРИФ по перевірці стану інформаційної безпеки. організації. 20. Критерії , порядок і методика перевірки політики безпеки за допомогою КОНДОР+. 21. Методи виявлення загроз функціонуванню підприємства. 22. Методи прогнозування загроз функціонуванню підприємства. 23. Методи оцінювання загроз та інформаційних ризиків. 24. Можливості моделей загроз безпеці систем і способів їх реалізації. 25. Підходи до визначення критеріїв уразливості і стійкості

			систем деструктивним впливам. 26. Вимірювання інформаційної безпеки. 27. Процес визначення метрик і їх оцінки відповідно до нормативних документів
Розділ 2 «РЕАЛІЗАЦІЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»			
Тема 3. ***Методологічні підходи до побудови систем управління інформаційною безпекою*** ***Знати***: концептуальний підхід до побудови ефективної системи інформаційної безпеки, вимоги забезпечення готовності організації до інцидентів інформаційної безпеки і безперервності діяльності організації. ***Вміти***: застосовувати процесний підхід до створення СУІБ і системи управління інцидентами інформаційної безпеки (СУІІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ за допомогою програми КОНДОР+, застосовувати метод аналізу ієрархій в системному аналізі інформаційної безпеки, реагувати на події ІБ за допомогою SIEM-систем з моніторингу подій. ***Формування компетенцій:*** ФК-7, ФК-8 ***Результати навчання:*** ПРН15,ПРН16,ПРН21, ПРН25, ПРН28-30 ***Рекомендовані джерела:*** 8,10,14, 15-20,30-42	Лекція 7	5,5*	Лекція-візуалізація
	Лекція 8		Лекція-візуалізація, експрес-опитування аспірантів
	Лекція 9		Лекція-візуалізація, експрес-опитування аспірантів
	Практичне заняття 13		Реалізація процесного підходу до побудови СУІБ - на прикладі. Обговорення результатів
	Практичне заняття 14		Застосування комбінованого підходу до створення СУІБ організації. Обговорення результатів
	Практичне заняття 15		Застосування підходу до створення СУІІБ організації. Обговорення результатів
	Практичне заняття 16		Застосування методу аналізу ієрархій у вирішенні задач інформаційної безпеки.
	Практичне заняття 17		Реалізація методики оцінки ефективності процесів управління подіями інформаційної безпеки в структурі SIEM-системи. Обговорення результатів
	Практичне заняття 18		Модульний контроль №2. Виконання кваліфікаційних завдань. Тестування
Тема 3. Методологічні підходи до побудови систем управління інформаційною безпекою	Самостійна робота		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. Вирішення задач за допомогою онлайн-программ. 20. Вирішення задач за допомогою Excel. 21. Практика моніторингу подій та реагування на події інформаційної безпеки. 22. Основні структури SIEM-систем з моніторингу подій інформаційної безпеки. 23. Підхід і методика оцінки ефективності процесу управління подіями інформаційної безпеки.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
- програмне забезпечення перевірки СУІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1 Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник. / В. Л. Бурячок, С. В.Толюпа, А. О. Аносов, В. А.Козачок, Н. В. Лукова-Чуйко. Київ: ДУТ, 2015. 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf.

2 Роїк О. М. Системний аналіз: навчальний посібник. /О. М. Роїк, А. А. Шиян, Л.О. Нікіфорова. Вінниця : ВНТУ, 2015. 83 с. URL: https://web.posibnyky.vntu.edu.ua/fmib/32royik_systemnyj_analiz/txt/zmist.html.

3 Якименко Ю. М. 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.

4 Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків. *Актуальні проблеми кібербезпеки:* матеріали Всеукраїн. наук. конф. (м. Київ, Україна, 27 жовтня 2021р.). Київ: ДУТ, 2021. С. 173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.
5 Якименко Ю. М. Підвищення ефективності системи менеджмента інформаційної безпеки організації. *Актуальні проблеми кібербезпеки*: матеріали II Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 27 жовтня 2022 р.). Київ: ДУТ, 2022. С. 198-200. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf.
6 Якименко Ю. М., Шилан А. О. Процесний підхід до управління безперервністю бізнесу на основі управління інформаційною безпекою. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:* матеріали конф. (м. Київ, Україна, 24 лютого 2022 р.). Київ: ДУТ, 2022. С. 7-12. URL: https://dut.edu.ua/uploads/p_2121_33783557.pdf.
7 Маркіна І. А. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва:* зб. наук. пр. 2016. № 3(1). С. 80-88. URL: http://nbuv.gov.ua/UJRN/piprp_2016_3(1)__18.
8 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.
9 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.
10 Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.
11 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.
12 Якименко Ю. М. Про підхід до створення системи інформаційної безпеки в організації. *Інформаційна безпека України*: зб. наук. доп. та тез НТК. (м. Київ, Україна, 23-24 березня 2017 р.). Київ: Київський національний університет імені Тараса Шевченка, 2017. С. 372-376.
13 Якименко Ю. М. Використання метрик для оцінки ефективності управління інциденту інформаційної безпеки. *Актуальні проблеми інформаційної та кібернетичної безпеки:* матеріали інтернет-конф. (м. Київ, Україна, 26 жовтня 2018 р.). Київ: ДУТ, 2018. С. 69-71.
14 Якименко Ю. М. Застосування системного підходу при організації захисту інформації. *Актуальні проблеми інформаційної та кібернетичної безпеки:* матеріали інтернет-конф. (м. Київ, Україна, 26 жовтня 2018 року). Київ: ДУТ, 2018. С. 44-45.
15 Якименко Ю. М. Особливості реалізації системного методу стосовно побудови систем управління інформаційною безпекою організації. *Актуальні проблеми управління інформаційною безпекою держави нові виклики та стратегії протидії:* матеріали X Всеукраїн. наук.-практ. конф. (м. Київ, Україна, 04 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 144-147. URL: https://academy.ssu.gov.ua/uploads/p_57_54325835.pdf.
16 Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою. *Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології*: матеріали IV Всеукр. Інтернет-конф. (м. Київ, Україна, 16 жовтня 2019 р.). за наук. ред. В.В. Сидоренко; упорядкування Я. Л. Швень, М. І. Скрипник. Київ: Агроосвіта, 2019. С. 41-43.
17 Якименко Ю. М. Огляд та оцінка стану кібербезпеки в умовах промислової революції (industry 4.0) в Україні. *Цифрова трансформація кібербезпеки:* матеріали конф. (м. Київ, Україна, 26 квітня 2020 р.). Київ: ДУТ, 2020. С. 5-6. URL: http://www.dut.edu.ua/uploads/p_1739_99516793.pdf.
18 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.
19 Якименко Ю. М. Управління інцидентами інформаційної безпеки в організації системи забезпечення кіберстійкості підприємства. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:* матеріали Всеукр. наук.-практ. конф. (м. Київ, Україна, 25 лютого 2021 р.). Київ: ДУТ, 2021. С. 24-25. URL: http://www.dut.edu.ua/uploads/l_2173_91341086.pdf.
20 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.
21 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:

22 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.

23 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.

24 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.

25 Якименко Ю. М. Вирішення проблеми забезпечення безперервності бізнесу завдяки впровадженню центру кіберстійкості *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:* матеріали ІІ 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.

26 Якименко Ю. М., Дьячук О. С. Методичний підхід до забезпчення безперервності бізнесу й відновлення після інциденту. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали ІІІ Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 23 лютого 2023 р.). Київ: ДУТ, 2023. С. 49-52.

27 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.

28 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.

29 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.

30 Akhramovych V., Shuklin G., Pepa Y., Lehominova S., Muzhanova T., Dzyuba T., Yakymenko Y. Methodology for Calculating the Index of Protection of a Social Media from its Centrality. *International Journal of Emerging Technology and Advanced Engineering*(IJETAE). 2023. Vol. 13. Issue 04. P. 17-25. (SCOPUS).

31 Tetiana M. Muzhanova, Yuriy M. Yakymenko, Mykhailo M. Zaporozhchenko, Vitalij S. Tyshchenko. International Vendor-Neutral Certification for Information Security Professionals. *Кібербезпека: освіта, наука, техніка*. 2022. № 4 (16). С. 129-141.

32 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.

33 ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. (ISO/IEC 27000:2018, IDT). (ДСТУ ISO/IEC 27000:2017).

34 ДСТУ ISO/IEC 27001:2015.(Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).

35 ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014).

36 ДСТУ ISO/IEC 27003:2018. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова. (ISO/IEC 27003:2017, IDT) (ISO/IEC 27003:2010).

37 ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ISO/IEC 27005:2018, IDT).

38 ДСТУ ISO/IEC 27007:2018. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою. (ISO/IEC 27007:2017, IDT).

39 ДСТУ ISO/IEC TS 27008:2019.Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. (ISO/IEC TS 27008:2019, IDT).

40 ДСТУ ISO/IEC 27009:2018. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги. (ISO/IEC 27009:2016, IDT).

41 ДСТУ ISO/IEC 27031:2015. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. (ISO/IEC 27031:2011, IDT).
42 ДСТУ ISO/IEC 27035-1:2018.Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки.Частина 1. Принципи керування інцидентами(ISO/IEC 27035-1:2016, IDT).
43 ДСТУ ISO/IEC 27035-1:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. (ISO/IEC 27035-1:2016, IDT).
44 ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).
45 ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).

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 практичних 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 аспірант 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 аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання аспірантом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «ВИМОГИ З ТЕОРІЇ УПРАВЛІННЯ СКЛАДНИМИ ПРОЦЕСАМИ ТА СИСТЕМАМИ»»	максимальна оцінка – 15балів
	Модульний контроль № 2 «РЕАЛІЗАЦІЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка –15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо.	Звільняється від екзамену

ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Аспірант 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 аспірант 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 аспіранта 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	Аспірант 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	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (В)

	занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.		
75-81	Аспірант 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)
64-74	Аспірант 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)
60-63	Аспірант 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, аспірант 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	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта 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*

1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі екзамену.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*