

## СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Системний аналіз інформаційної безпеки»

<b>Лектор курсу</b>			<b>Якименко Юрій Михайлович</b> , кандидат військових наук, доцент, доцент кафедри “Управління інформаційною та кібернетичною безпекою”		<b>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</b>		<b>e-mail:</b> <a href="mailto:yakum14@ukr.net">yakum14@ukr.net</a> ; <b>сторінка курсу в Moodle –</b> <a href="https://dn.dut.edu.ua/course/view.php?id=397">https://dn.dut.edu.ua/course/view.php?id=397</a>	
<b>Галузь знань</b>			12 Інформаційні технології		<b>Рівень вищої освіти</b>		перший (бакалавр)	
<b>Спеціальність</b>			125 Кібербезпека		<b>Семестр</b>		5	
<b>Освітня програма</b>			КІБЕРБЕЗПЕКА		<b>Тип дисципліни</b>		загальної підготовки	
<b>Обсяг:</b>	Кредитів ECTS	Годин	За видами занять:					
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
	5	150	36	-	36	-	78	

### АНОТАЦІЯ КУРСУ

**Мета курсу:** формування у студентів базових теоретичних знань, умінь і практичних навичок, необхідних для використання системного підходу, використанню обчислювальних засобів для вирішення задач аналізу та синтезу складних систем у сфері інформаційної безпеки.

#### Компетентності відповідно до освітньої програми

##### Soft- skills / Загальні компетентності (ЗК)

**ЗК1.** Здатність застосовувати знання у практичних ситуаціях.  
**ЗК5.** Здатність до пошуку, оброблення та аналізу інформації.

##### Hard-skills / Фахові компетентності (ПП)

**ПП 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.  
**ПП 10.** Здатність застосовувати методи та засоби захисту інформації на об'єктах інформаційної діяльності.

#### Програмні результати навчання (ПРН)

**ПРН 1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.  
**ПРН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки.  
**ПРН 10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.  
**ПРН 46.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів захисту інформації.  
**ПРН 47.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

### ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
-----------------	----------------	-----------------------	---

## Розділ 1 «ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ СИСТЕМ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

<p>Тема 1. <b>Впровадження теорії систем управління в інформаційні системи організації</b></p> <p><b>Знати:</b> стан розвитку теорії систем та її елементи, сприйняття організації як предмет для дослідження, класифікацію інформаційних систем управління, інформаційно-аналітичні системи (ІАС), нормативну базу розробки та впровадження систем управління інформаційною безпекою (СУІБ)</p> <p><b>Вміти:</b> класифікувати інформаційні системи підприємств, використовувати підходи до побудови їх систем управління і оцінювати ефективність управлінських рішень організацією.</p> <p><b>Формування компетенцій:</b>ЗК1, ЗК5, ПП1</p> <p><b>Результати навчання:</b>ПРН7, ПРН10</p> <p><b>Рекомендовані джерела:</b> 1,2,5,6,7, 10</p>	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Лекція 3		Лекція-візуалізація
	Лекція 4		Лекція-візуалізація, експрес-опитування студентів
	Лекція 5		Лекція-візуалізація
	Практичне заняття 1		Вирішення задачі по класифікації систем підприємств на прикладі. Обговорення результатів
	Практичне заняття 2		Вирішення задачі побудови організаційної структури підприємства і її системи управління на прикладі. Обговорення результатів
	Практичне заняття 3		Оцінка ефективності управлінських рішень організацією на прикладі. Обговорення результатів
Практичне заняття 4	Усне опитування, навчальна дискусія, доповідь з презентацією за темою Нормативні документи з питань безпеки комп'ютерних систем в США		
<p>Тема 2. <b>Методологічні підходи до побудови та дослідження систем управління інформаційною безпекою</b></p> <p><b>Знати:</b> методологічні підходи до дослідження систем управління інформаційною безпекою, методи та засоби інформаційних технологій для вирішення задач системного аналізу і управління в області комп'ютерних систем, загальні проблеми безпеки інформаційних систем та багаторівневий підхід до забезпечення їх інформаційної безпеки, вимоги по стандартизації до систем і процесів управління інформаційною безпекою та впровадження системи управління інформаційною безпекою, підходи до застосування ситуаційного підходу в системах управління, підхід до розробки та впровадженню системи управління інцидентами інформаційної безпеки (СУІБ);</p> <p>методику впровадження процесного підходу до створення СУІБ</p>	Лекція 6	5,5*	Лекція-візуалізація
	Лекція 7		Лекція-візуалізація, експрес-опитування студентів
	Лекція 8		Лекція-візуалізація
	Лекція 9		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 6		Впровадження процесного підходу до створення СУІБ на прикладі. Обговорення результатів

<p>організації та СУІБ, нормативні вимоги до СУІБ з управління ризиками ІБ (відповідно до стандартів ISO / ІЕС 2700-к); алгоритм прийняття управлінських рішень по вирішенню проблем з ІБ.</p> <p><b>Вміти:</b> впроваджувати методологічні підходи до побудови та дослідження систем управління інформаційною безпекою: СУІБ, СУІБ і системи управління ризиками ІБ, використовувати методи та засоби інформаційних технологій для вирішення задач системного аналізу процесів і систем управління.</p> <p><b>Формування компетенцій:</b>ЗК1, ПП1, ПП10</p> <p><b>Результати навчання:</b> ПРН7,ПРН10, ПРН46</p> <p><b>Рекомендовані джерела:</b> 1,2,5, 7–10,13,14-17</p>	Практичне заняття 7	Впровадження системного підходу до побудови СУІБ на прикладі. Обговорення результатів
	Практичне заняття 8	Впровадження процесного підходу до створення СУІБ на прикладі. Обговорення результатів
	Практичне заняття 9	Модульний контроль №1. Виконання кваліфікаційних завдань. Тестування
<p><b>Тема 1.</b> Основні положення теорії систем у сфері ІБ</p> <p><b>Тема 2.</b> Методологічні підходи до побудови та дослідження систем управління ІБ</p>	Самостійна робота	<ol style="list-style-type: none"> <li>1. Основні поняття та принципи загальної теорії систем і системного аналізу</li> <li>2. Види систем та особливості їх функціонування</li> <li>3. Особливості організаційно-технічних систем</li> <li>4. Система управління організації</li> <li>5. Можливості інформаційних систем MIS та DSS</li> <li>6. Підходи до побудови систем на базі OLAP-технологій, функції та сфери їх застосування</li> <li>7. Варіанти архітектури сховищ даних в ІАС та їх можливості</li> <li>8. Класифікація систем і побудова організаційних структур підприємств</li> <li>9. Методика оцінки ефективності управлінських рішень</li> <li>10. Міжнародні документи в галузі інформаційної безпеки</li> <li>11. Нормативні документи з питань безпеки комп'ютерних систем в США</li> <li>12. Методологічні підходи до дослідження систем управління</li> <li>13. Підхід до побудови захисту інформації у корпоративній інформаційній системі</li> <li>14. Застосування процесного підходу до створення СУІБ організації</li> <li>15. Ситуаційний підхід в дослідженні систем управління</li> <li>16. Застосування підходу до створення СУІБ організації</li> <li>17. Особливості застосування системного підходу до побудови СУІБ</li> <li>18. Комбінований підхід в процесах управління ІБ</li> <li>19. Методика обґрунтування прийнятих управлінських рішень з безпеки в організації</li> </ol>

**Розділ 2 «РЕАЛІЗАЦІЯ МЕТОДОЛОГІЧНИХ ПІДХОДІВ У СИСТЕМНОМУ АНАЛІЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»**

<p>Тема 3. <b>Основи системного аналізу інформаційної безпеки</b>  <b>Знати:</b> технології системного аналізу та їх застосування на практиці, основні принципи та підходи до системного аналізу, методи дослідження інформаційних систем в системному аналізі, аналіз та синтез як методи дослідження і проектування організацій; метод експертних оцінок в системному аналізі; методика застосування і можливості програм методу аналізу ієрархій (MAI) у вирішенні управлінських задач; порядок рішення задач побудови мережевих моделей в системному аналізі; методика оцінки економічної безпеки підприємства;</p> <p><b>Вміти:</b> вирішувати задачі дослідження з використанням програмних продуктів MAI в системному аналізі, вирішувати задачі побудови мережевих моделей в системному аналізі, моделювати структуру дослідження і використовувати методологічні підходи до оцінки економічної безпеки підприємства.</p> <p><b>Формування компетенцій:</b> ЗК1, ПП1, ПП10  <b>Результати навчання:</b> ПРН10, ПРН46  <b>Рекомендовані джерела:</b> 2,4-6,7,9,</p>	Лекція 10	5,5*	Лекція-візуалізація
	Лекція 11		Лекція-візуалізація, експрес-опитування студентів
	Лекція 12		Лекція-візуалізація
	Лекція 13		Лекція-візуалізація, експрес-опитування студентів
	Лекція 14		Лекція-візуалізація
	Практичне заняття 10		Вирішення задачі дослідження з використанням програмних продуктів MAI на прикладі
	Практичне заняття 11		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 12		Вирішення задачі дослідження з використанням програмних продуктів по побудові мережевого графіка на прикладі
Практичне заняття 13	Вирішення задачі дослідження з використанням програмних продуктів оцінки економічної безпеки на прикладі		
<p>Тема 4. <b>Моделювання у системному аналізі інформаційної безпеки</b>  <b>Знати:</b> підходи до моделювання процесів створення і оцінки ефективності систем захисту інформації, сучасні методи й моделі обґрунтування та прийняття рішень, підходи до організації моніторингу безпеки в інформаційній системі, методика проведення аудиту інформаційної безпеки інформаційних та комп'ютерних систем; вимоги стандартів ISO та можливості застосування програм Cobra і КОНДОР+ для перевірки СУІБ на відповідність вимогам стандартів ISO; особливості оцінки загроз та інформаційних ризиків і методика оцінки ІБ з використанням методу SWOT- аналізу; можливості програмних продуктів SIEM у вирішенні задачі управління подіями ІБ</p>	Лекція 15	5,5*	Лекція-візуалізація
	Лекція 16		Лекція-візуалізація, експрес-опитування студентів
	Лекція 17		Лекція-візуалізація
	Лекція 18		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 14		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 15		Вирішення задачі перевірки СУІБ з використанням програмних продуктів на прикладі

<p><b><u>Вміти:</u></b> вирішувати задачі перевірки СУІБ на відповідність вимогам стандартів ISO, використовувати метод SWOT- аналізу в оцінці інформаційної безпеки, використовувати програмні продукти SIEM в системі управління подіями інформаційної безпеки.</p> <p><b><u>Формування компетенцій:</u></b>ЗК5, ПП10</p> <p><b><u>Результати навчання:</u></b> ПРН10, ПРН46</p> <p><b><u>Рекомендовані джерела:</u></b> 1,3,6,8-10,18</p>	Практичне заняття 16		Вирішення задачі оцінки інформаційної безпеки з використанням програмних продуктів на прикладі
	Практичне заняття 17		Використання можливостей програмного продукту SIEM у вирішенні задачі управління подіями ІБ на прикладі
	Практичне заняття 18		Модульний контроль №2. Виконання кваліфікаційних завдань. Тестування
<p><b>Тема 3.</b> Основи системного аналізу інформаційної безпеки</p> <p><b>Тема 4.</b> Моделювання у системному аналізі інформаційної безпеки</p>	Самостійна робота		<ol style="list-style-type: none"> <li>1. Основні різновиди системного аналізу</li> <li>2. Структура аналізу та методологія системного аналізу</li> <li>3. Системний аналіз інформаційних систем</li> <li>4. Закон єдності аналізу і синтезу</li> <li>5. Цілі, завдання аналізу і синтезу систем управління</li> <li>6. Застосування методу експертної оцінки в системному аналізі</li> <li>7. Можливості програм методу аналізу ієрархій у вирішенні управлінських задач</li> <li>8. Застосування мережевого графіка в системному аналізі</li> <li>9. Основні показники оцінки економічної безпеки підприємства</li> <li>10. Моделі та моделювання систем</li> <li>11. Технології підтримки та прийняття рішень</li> <li>12. Моніторинг інформаційної безпеки організації</li> <li>13. Аудит інформаційної безпеки організації</li> <li>14. Методика проведення інструментальних перевірок</li> <li>15. Практика проходження перевірки СУІБ на відповідність вимогам стандартів ISO</li> <li>16. Використання методу SWOT- аналізу в оцінці інформаційної безпеки</li> <li>17. Використання IBM QRadar SIEM в системі управління подіями інформаційної безпеки</li> <li>18. Системи управління базами даних та освоєння роботи з таблицями в Microsoft Access</li> <li>19. Методики роботи в СУБД ACCESS по питанням: створення запитів, форм та звітів</li> </ol>
<b>МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ</b>			
<ul style="list-style-type: none"> <li>• мультимедійна система Acer X113 DLP</li> <li>• комп'ютери Asus</li> <li>• комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».</li> </ul>			

- програмне забезпечення: засоби підтримки прийняття рішень у сфері ІБ

## 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 / – К.:ДУТ, 2015. – 345 с. URL: [http://www.dut.edu.ua/uploads/l\\_1242\\_54311567.pdf](http://www.dut.edu.ua/uploads/l_1242_54311567.pdf)  
<https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd>.
2. Роїк О. М. Системний аналіз. Навчальний посібник / О. М. Роїк, А. А. Шиян, Л.О. Нікіфорова – Вінниця : ВНТУ, 2015. – 83 с. URL: <http://nikiforova.vk.vntu.edu.ua/file/bfb63146b18f718fe1ff1ed4ce9b9a58.pdf>.
3. Рой Я.В., Мазур Н.П., Складанні П.М.Аудит інформаційної безпеки –основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/23>
4. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою.- Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології: програма ІУ-ої Всеукраїнської Інтернет-конференції 16 жовтня 2019 р., м. Київ.-/ за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. К.: Агроосвіта, 2019.- С.41-43.
5. Данілова Е.І. Концепція системного підходу до управління економічною безпекою підприємства. Монографія. Вінниця: Європейська наукова платформа, 2020. 342с. URL: <https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859>
6. Грецька Г. М. Конспект лекцій з курсу «Теорія систем і системний аналіз»/ Г. М. Грецька: Харк. нац. акад. міськ. госп-ва. - Х.: ХНАМГ. 2011. - 148 с.
7. Пеклун К. В. Теорія систем і системний аналіз. Одеса: ОРІДУ НАДУ при Президентіві України, 2013. URL: <http://oridu.odessa.ua/7/7/pdf/6.pdf>.
8. Побудова Системи управління інформаційною безпекою (СУІБ). URL: <https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/>.
9. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: [https://www.dut.edu.ua/uploads/l\\_2230\\_88161692.pdf](https://www.dut.edu.ua/uploads/l_2230_88161692.pdf)
10. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – К. : Університет «Україна», 2013. – 203 с. URL: <http://er.nau.edu.ua/handle/NAU/20105> , <http://er.nau.edu.ua:8080/handle/NAU/20105>.
11. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
12. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014), Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
13. ДСТУ ISO/IEC 27003:2018 ( ISO/IEC 27003:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова . (ISO/IEC 27003:2010)
14. ДСТУ ISO/IEC 27009:2018 (ISO/IEC 27009:2016, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги
15. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ДСТУ ISO/IEC 27005:2015)
16. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки
17. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами.
18. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT)Настанови щодо проведення аудитів систем управління
19. ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) Менеджмент ризиків. Принципи та настанови

## 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 студент 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 студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, 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 студент видаляється з заняття, за заняття отримує 0 балів.

### \*КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

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

Форми контролю	Види навчальної роботи	Оцінювання
<b>ПОТОЧНИЙ КОНТРОЛЬ</b>	<i>Робота на заняттях, у т.ч.:</i>	
	• 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
<b>РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)</b>	Модульний контроль № 1 «ВИРШЕННЯ ЗАДАЧ СИСТЕМНОГО АНАЛІЗУ ПРОЦЕСІВ І СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «РЕАЛІЗАЦІЯ МЕТОДОЛОГІЧНИХ ПІДХОДІВ У СИСТЕМНОМУ АНАЛІЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 15 балів
<b>Додаткова оцінка</b>	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
<b>ПІДСУМКОВЕ ОЦІНЮВАННЯ</b> <i>Іспит</i>	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 /затис в екзаменаційній відомості
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях.	<b>Високий</b> Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій	Відмінно / Зараховано (А)

	<p>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.</p> <p>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 студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.</p>	<p>програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.</p>	
82-89	<p>Студент 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.</p> <p>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.</p>	<p><b>Достатній</b> Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни</p>	<p>Добре / Зараховано (B)</p>
75-81	<p>Студент 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.</p>	<p><b>Достатній</b> Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.</p>	<p>Добре / Зараховано (C)</p>
64-74	<p>Студент 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 розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.</p>	<p><b>Середній</b> Забезпечує достатньо надійний рівень відтворення основних положень дисципліни</p>	<p>Задовільно / Зараховано (D)</p>
60-63	<p>Студент 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, студент 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.</p>	<p><b>Середній</b> Є мінімально допустимим у всіх складових навчальної програми з дисципліни</p>	<p>Задовільно / Зараховано (E)</p>
35-59	<p>Студент може відтворити окремі фрагменти з курсу.</p> <p>Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими.</p>	<p><b>Низький</b> Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни</p>	<p>Незадовільно з можливістю повторного складання)</p>



	Цілісність розуміння матеріалу з дисципліни у студента відсутні.		/ Не зараховано (FX) В залікову книжку не представляється
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	<b>Незадовільний</b> Студент 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 представляється