СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Системний аналіз інформаційної безпеки»

Лектор курсу			**Якименко Юрій Михайлович**, кандидат військових наук, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою **Савченко Віталій Анатолійович**, доктор технічних наук, професор, директор Навчально-наукового інституту захисту інформації.		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**yakum14@ukr.net; **сторінка курсу в Moodle – https://dn.dut.edu.ua/course/view.php?id=413**	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	третій (освітньо-науковий) - доктор філософії	
Спеціальність			125 Кібербезпека		**Семестр**	1	
Освітня програма			КІБЕРБЕЗПЕКА		**Тип дисципліни**	вибірковий компонент ОНП	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	формування базових теоретичних знань, умінь і практичних навичок, необхідних для використання системного підходу, його принципів і методів у дослідженні складних організаційно-технічних систем на об'єктах інформаційної діяльності і в управлінні 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). **ПРН-15** 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**
Розділ 1 «ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ СИСТЕМ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 1. ***Впровадження теорії систем управління в інформаційні системи організації*** ***Знати***: 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) ***Вміти:*** класифікувати інформаційні системи підприємств, використовувати підходи до побудови їх систем управління і оцінювати ефективність управлінських рішень організацією. ***Формування компетенцій:***ЗК1, ЗК5, ПП1 ***Результати навчання:***ПРН7, ПРН10 ***Рекомендовані джерела:*** 1,2,5,6,7, 10	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 1		Вирішення задачі по класифікації систем та з побудовою організаційної структури підприємства і її системи управління на прикладі. Обговорення результатів
	Практичне заняття 2		Оцінка ефективності управлінських рішень організацією на прикладі. Обговорення результатів
Тема 2. ***Методологічні підходи до побудови та дослідження систем управління інформаційною безпекою*** ***Знати***: 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 (СУІІБ); методику впровадження процесного підходу до створення СУІБ організації та СУІІБ, нормативні вимоги до СУІБ з управління ризиками ІБ (відповідно до стандартів ISO / IEC 2700-к); алгоритм прийняття управлінських рішень по проблемам з ІБ.	Лекція 3	5,5*	Лекція-візуалізація
	Лекція 4		Лекція-візуалізація, експрес-опитування студентів
	Лекція 5		Лекція-візуалізація
	Практичне заняття 3		Впровадження системного підходу до побудови СУІБ на прикладі. Обговорення результатів

Вміти: впроваджувати методологічні підходи до побудови та дослідження систем управління інформаційною безпекою: СУІБ, СУІІБ і системи управління ризиками ІБ, використовувати методи та засоби інформаційних технологій для вирішення задач системного аналізу процесів і систем управління. ***Формування компетенцій:***ЗК1, ПП1, ПП10 ***Результати навчання:*** ПРН7,ПРН10, ПРН46 ***Рекомендовані джерела:*** 1,2,5, 7–10,13,14-17	Практичне заняття 4		Впровадження процесного підходу до створення СУІІБ на прикладі. Обговорення результатів Модульний контроль №1. Виконання кваліфікаційних завдань. Тестування
Тема 1. Основні положення теорії систем у сфері ІБ **Тема 2.** Методологічні підходи до побудови та дослідження систем управління ІБ	Самостійна робота		1. Основні поняття та принципи загальної теорії систем і системного аналізу 2. Види систем та особливості їх функціонування 3. Особливості організаційно-технічних систем 4. Система управління організації 5. Можливості інформаційних систем MIS та DSS 6. Підходи до побудови систем на базі OLAP-технологій, функції та сфери їх застосування 7. Варіанти архітектури сховищ даних в ІАС та їх можливості 8. Класифікація систем і побудова організаційних структур підприємств 9. Методика оцінки ефективності управлінських рішень 10. Міжнародні документи в галузі інформаційної безпеки 11. Нормативні документи з питань безпеки комп'ютерних систем в США 12. Методологічні підходи до дослідження систем управління 13. Підхід до побудови захисту інформації у корпоративній інформаційній системі 14. Застосування процесного підходу до створення СУІБ організації 15. Ситуаційний підхід в дослідженні систем управління 16. Застосування підходу до створення СУІІБ організації 17. Особливості застосування системного підходу до побудови СУІБ 18. Комбінований підхід в процесах управління ІБ 19. Методика обгрунтування прийнятих управлінських рішень з безпеки в організації
Розділ 2 «РЕАЛІЗАЦІЯ МЕТОДОЛОГІЧНИХ ПІДХОДІВ У СИСТЕМНОМУ АНАЛІЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			

Тема 3. ***Основи системного аналізу інформаційної безпеки*** ***Знати***: 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; методику застосування і можливості програм методу аналізу ієрархій (MAI) у вирішенні управлінських задач; порядок рішення задач побудови мережевих моделей в системному аналізі; методику оцінки економічної безпеки підприємства; ***Вміти***: 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. ***Формування компетенцій:*** ЗК1, ПП1, ПП10 ***Результати навчання:*** ПРН10, ПРН46 ***Рекомендовані джерела:*** 2,4-6,7,9	Лекція 6	5,5*	Лекція-візуалізація
	Лекція 7		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Вирішення задачі дослідження з використанням програмних продуктів MAI на прикладі
	Практичне заняття 6		Вирішення задачі дослідження з використанням програмних продуктів по побудові мережевого графіка на прикладі
Тема 4. ***Моделювання у системному аналізі інформаційної безпеки*** ***Знати***: 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, методику 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 методику оцінки ІБ з використанням методу SWOT- аналізу; можливості програмних продуктів SIEM у вирішенні задачі управління подіями ІБ	Лекція 8	5,5*	Лекція-візуалізація
	Лекція 9		Лекція-візуалізація, експрес-опитування студентів

Вміти: 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. ***Формування компетенцій:***ЗК5, ПП10 ***Результати навчання:*** ПРН10, ПРН46 ***Рекомендовані джерела:*** 1,3,6,8-10,18	Практичне заняття 7		Вирішення задачі перевірки СУІБ з використанням програмних продуктів на прикладі
	Практичне заняття 8		Використання можливостей програмного продукту SIEM у вирішенні задачі управління подіями ІБ на прикладі.
	Практичне заняття 9		Модульний контроль №2. Виконання кваліфікаційних завдань. Тестування
Тема 3. Основи системного аналізу інформаційної безпеки **Тема 4.** Моделювання у системному аналізі інформаційної безпеки	Самостійна робота		1. Основні різновиди системного аналізу 2. Структура аналізу та методологія системного аналізу 3. Системний аналіз інформаціонних систем 4. Закон єдності аналізу і синтезу 5. Цілі, завдання аналізу і синтезу систем управління 6. Застосування методу експертної оцінки в системному аналізі 7. Можливості програм методу аналізу ієрархій у вирішенні управлінських задач 8. Застосування мережевого графіка в системному аналізі 9. Основні показники оцінки економічної безпеки підприємства 10. Моделі та моделювання систем 11. Технології підтримки та прийняття рішень 12. Моніторинг інформаційної безпеки організації 13. Аудит інформаційної безпеки організації 14. Методика проведення інструментальних перевірок 15. Практика проходження перевірки СУІБ на відповідність вимогам стандартів ISO 16. Використання методу SWOT- аналізу в оцінці інформаційної безпеки 17. Використання IBM QRadar SIEM в системі управління подіями інформаційної безпеки 18. Системи управління базами даних та освоєння роботи з таблицями в Microsoft Access 19. Методики роботи в СУБД ACCESS по питанням: створення запитів, форм та звітів

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: 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 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., Складанний 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. Пєклун К. В. Теорія систем і системний аналіз. Одеса: ОРІДУ НАДУ при Президентові України, 2013. URL: http://oridu.odessa.ua/7/7/pdffile/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
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
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 «ВИРІШЕННЯ ЗАДАЧ СИСТЕМНОГО АНАЛІЗУ ПРОЦЕСІВ І СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «РЕАЛІЗАЦІЯ МЕТОДОЛОГІЧНІИХ ПІДХОДІВ У СИСТЕМНОМУ АНАЛІЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку 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	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. 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 студент 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 студента 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 (A)
82-89	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. 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 студенту 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	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.	**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	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 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	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	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

	відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.		
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента 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	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	**Незадовільний** 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 проставляється*