СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «АУДИТ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Запорожченко Михайло Михайлович, асистент кафедри управління інформаційною та кібернетичною безпекою</td><td>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: zaporozhchenkomm@gmail.com; сторінка курсу в Moodle – http://dn.dut.edu.ua/course/view.php?id=395</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 «Інформаційні технології»</td><td>Рівень вищої освіти</td><td colspan="2">бакалавр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">125 «Кібербезпека та захист інформації»</td><td>Семестр</td><td colspan="2">7</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">«Управління інформаційною та кібернетичною безпекою»</td><td>Тип дисципліни</td><td colspan="2">Вибіркова</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>5</td><td>150</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
36</td><td>Лабораторних занять
-</td><td>Самостійна підготовка
96</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">формування у студентів необхідної системи знань з основ аудиту систем захисту інформації.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Фахові компетенції</td></tr>
<tr><td colspan="4">ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.</td><td colspan="4">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 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.
ПП 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем.
ПП 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресур</td></tr>
<tr><td colspan="8">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="8">ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 7. Діяти на основі законодавчої та нормативноправової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 18. Використовувати програмні та програмноапаратні комплекси захисту інформаційних ресурсів.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних</td></tr>
</table>

(автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.
ПРН 29. Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
ЗМІСТОВИЙ МОДУЛЬ 1 "МОЖЛИВОСТІ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БАЗОВІ ПОНЯТТЯ З АУДИТУ ЇХ ФУНКЦІОНУВАННЯ"			
Тема 1. ***Загальні відомості щодо функціонування систем менеджменту інформаційної безпеки та проведення їх аудиту*** ***Знати***: основні завдання систем захисту інформації, особливості використання програмних та апаратних систем захисту інформації, загальні особливості проведення аудиту систем захисту інформації, знати цілі і завдання проведення аудиту, види аудитів та характеристики внутрішніх аудитів, знати принципи проведення внутрішнього аудиту. ***Вміти***: проводити роботи з оцінки характеристик автоматизованої системи та мов її функціонування, уміти аналізувати систему захисту інформації на її відповідність Політиці безпеки інформації. ***Формування компетенцій:*** ЗК 1, ЗК 2, ЗК 4, ЗК 5, ПП 1 ***Результати навчання:*** ПРН 3, ПРН 6, ПРН 7, ПРН 28 ***Рекомендовані джерела:*** *1-19*	Лекція 1 2 год	5,5*	Лекція-візуалізація
	Практичне заняття 1 4 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 2 2 год		Лекція-візуалізація
	Практичне заняття 2 4 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Тема 2. ***Принципи та процедури аудиту систем менеджменту інформаційної безпеки. Етапи проведення аудиту*** ***Знати***: Основні поняття аудиту, їх типи, цілі та критерії аудитів, осіб, яких необхідно залучити до проведення аудитів та принципи проведення аудитів, обов'язки аудиторів, підходи до аудитів на основі доказів та ризиків, типи та якість аудиторських доказів. Перелік заходів, виконання яких є необхідним на етапі ініціювання аудиту, цілі 1 та 2 етапів аудиту, вимоги до підготовки робочих документів, призначення аудиторів, створення планів тестування при аудиті, особливості проведення вступної зустрічі, збору інформації, проведення аудиторських тестів згідно з відповідними процедурами, принципи розробки тестових планів аудиту, типи можливих результатів аудиту, вимоги до редакції результатів аудиту та звіту про	Лекція 3 2 год	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3 4 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 4 2 год		Лекція-візуалізація, експрес-опитування студентів

невідповідність, робочі документи та протоколи аудиту, процедури завершення аудиту. ***Вміти***: визначати цілі та критерії аудитів, класифікувати їх за типами, класифікувати та визначати якість аудиторських доказів, застосовувати підходи до аудитів на основі доказів та ризиків, аналізувати заявки на аудит, визначати можливість виконання аудиту, підбирати аудиторів до команди, формувати план аудиту, створювати плани тестування при аудитах, підготовлювати робочі документи, використовувати контрольні списки, збирати необхідну інформацію для проведення аудиту, проводити аудиторські тести, виявляти недоліки та невідповідності та в подальшому заносити їх до звіту, розроблювати плани тестування при проведенні аудитів, визначати результати аудиту, визначати аудиторські висновки, застосовувати на практиці процедури завершення аудиту. ***Формування компетенцій:*** ЗК 1, ЗК 2, ЗК 4, ЗК 5, ПП 1, ПП 9 ***Результати навчання:*** ПРН 3, ПРН 4, ПРН 6, ПРН 7, ПРН 15, ПРН 28 ***Рекомендовані джерела:*** *1-19*	Практичне заняття 4 4 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 5 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5 4 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 6 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 6 4 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Тема 1. ***Загальні відомості щодо функціонування систем менеджменту інформаційної безпеки та проведення їх аудиту*** Тема 2. ***Принципи та процедури аудиту систем менеджменту інформаційної безпеки. Етапи проведення аудиту***	Самостійна робота		1. Міжнародні стандарти щодо заходів управління інформаційною безпекою 2. Характеристики захищеності інформаційних ресурсів 3. Модель CIA. Задачі забезпечення цілісності, доступності та конфіденційності 4. Політика кібербезпеки інформації та модель порушника. 5. Загрози безпеці державних інформаційних ресурсів. 6. Типові уразливості інформаційних та комунікаційних систем, причини їх появи. 7. Загрози інформації та вибір функціонального класу послуг захисту 8. Критерії оцінки рівня інформаційної безпеки за національними стандартами 9. Критерії оцінки рівня інформаційної безпеки за міжнародними стандартами 10. Особливості проведення внутрішнього та зовнішнього аудитів. 11. Проведення аудиту на відповідність вимогам стандартів.

			12. Класифікація заходів захисту. 13. Види процедур збору інформації при проведенні аудитів. 14. Активний аудит. 15. Зміст звіту про аудит. 16. Аналіз ризиків при проведенні аудиту. 17. Вимоги до кваліфікації аудитора. 18. Рекомендації з вдосконалення як складова звіту аудиту.
ЗМІСТОВИЙ МОДУЛЬ 2 "ПРОВЕДЕННЯ АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ПРОГРАМНИХ ТА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ"			
Тема 3. ***Інструментальний аудит захищеності автоматизованих систем*** ***Знати***: Знати етапи проведення робіт з інвентаризації ресурсів мережі (пристроїв, операційних систем, служб, програмного забезпечення), знати особливості проведення ідентифікації та аналізу технологічних вразливостей, знати вимоги до підготовки звітів опису проблем і методів усунення, аналіз VPN-шлюзів з точки зору захисту інформації, аналіз антивірусних засобів захисту, системи захисту операційних систем сімейства Windows, можливості штатних засобів моніторингу та аудиту, системи захисту від несанкціонованого доступу операційних систем сімейства UNIX, штатні засоби моніторингу та аудиту, базові принципи систем виявлення атак IDS/IPS, можливості міжмережевих екранів, можливості систем захисту від витоку конфіденційної інформації, методи ідентифікації інформаційних активів, вимоги до формування каталогу можливих загроз безпеки інформації та оцінки ймовірності їх реалізації. ***Вміти***: використовувати програмні засоби аудиту систем захисту інформації, використовувати програмно-апаратні засоби аудиту систем захисту, знати можливості та уміти використовувати програмні засоби моніторингу систем захисту баз даних, проводити аудит налаштувань Bios та первинної ініціалізації операційної системи, проводити роботи з конфігурування параметрів безпеки ОС, аналізувати стан безпеки комутаторів та маршрутизаторів, проводити оцінку безпеки WLAN і SAN-мереж, використовувати засоби виявлення інформації з обмеженим доступом в автоматизованій системі, проводити пошук інформації з обмеженим доступом в мережі інтернет, проводити оцінку та аналіз можливостей програмних рішень моніторингу, проводити налаштування програм-клієнтів моніторингу стану системи захисту інформації, аналізувати ризики безпеки систем захисту інформації, які були виявлені в ході проведення аудиту,	Лекція 7 2 год	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 7 4 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 8 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 8 4 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 9 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9 4 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання

розробляти рекомендації по вдосконаленню систем захисту інформації. ***Формування компетенцій:*** ЗК 1, ЗК 2, ЗК 4, ЗК 5, ПП 1, ПП 9, ПП 11 ***Результати навчання:*** ПРН 3, ПРН 6, ПРН 7, ПРН 15, ПРН 18, ПРН 28, ПРН 29 ***Рекомендовані джерела:*** *1-19*			
Тема 3. ***Інструментальний аудит захищеності автоматизованих систем***	Самостійна робота		1. Загальні правила управління безпекою підприємства 2. Система управління інформаційною безпекою 3. Функції технологічного управління інформаційною безпекою 4. Загальні положення з управління інформаційною безпекою 5. Загальні принципи аудиту інформаційної безпеки 6. Цілі та метод проведення аудиту 7. Класифікація типів системи виявлення та блокування атак 8. Концепція та система автоматизованої обробки інцидентів безпеки на мережевому рівні 9. Організація служби інформаційної безпеки підприємства 10. Категорії інформації, що збирається для аналізу атак 11. Методи виявлення інформаційних атак

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.
- Перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій та слайдів до лекцій через систему MOODLE для підготовки до практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Рекомендовані джерела та інші навчальні ресурси:

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України редакція від 04 липня 2020 р. № 80/94-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
2. Про основні засади забезпечення кібербезпеки України : Закон України редакція від 24 жовтня 2020 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3 Про національну безпеку України : Закон України редакція від 24 жовтня 2020 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355
4. Про заходи щодо захисту інформаційних ресурсів держави : Указ Президента України №582/2000 від 10.04 2000 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/582/2000#Text.
5. НД ТЗІ 3.1-003-2005. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ

України від 24.04.1999 р. № 22 Чинний від 01.07.1999 р. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf
8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53 Чинний від 15.12.2000 р. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf
9. Інформаційна безпека інформаційно-комунікаційних систем. Комплекси засобів захисту інформації від НСД. URL: http://www.dut.edu.ua/uploads/l_489_79827499.pdf
10. 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
11. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою
12. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT) Настанови щодо проведення аудитів систем управління
13. Інформаційні технології в бізнесі. Частина 1: Навч. посіб. / [Шевчук І.Б., Старух А.І., Васьків О.М. та ін.]; за заг. ред. І.Б. Шевчук. Львів: Видавництво ННВК «АТБ», 2020. 455 с. URL: https://financial.lnu.edu.ua/wp-content/uploads/2020/11/Posibnyk_IT-v-biznesi_2.pdf
14. Manual of Information Technology Audit. URL: https://cag.gov.in/uploads/media/ITAM-Vol-I-20210331113105.pdf
15. Information Security Audit (IT Audit / IS Audit). URL: https://youtu.be/fQefScHAs6A
16. Day 3: Security Auditing and Compliance. URL: https://youtu.be/O_noXhQ16Yk
17. Learn how to become great Cybersecurity Auditors and Consultants. URL: https://youtu.be/R6p4m5TGgik
18. How to Perform an Internal Network Audit. URL: https://youtu.be/-REmXQKzcCw
19. How to carry out an IT Infrastructure Audit. URL: https://youtu.be/kHkCNi0B4VY

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 40 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 балу
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 балу
	• 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 балу
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «МОЖЛИВОСТІ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БАЗОВІ ПОНЯТТЯ З АУДИТУ ЇХ ФУНКЦІОНУВАННЯ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «ПРОВЕДЕННЯ АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ПРОГРАМНИХ ТА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ»	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. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в заліковій 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 (А)
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 (В)
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/	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для	Добре / Зараховано (С)

	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.	практичного використання викликають утруднення.	
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 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	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*