СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«МЕТОДОЛОГІЯ НАУКОВИХ ДОСЛІДЖЕНЬ У КІБЕРБЕЗПЕЦІ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="3">Гайдур Галина Іванівна, доктор технічних наук, професор, завідувач кафедри Систем та технологій кібербезпеки</td><td>Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: g.haidur@duikt.edu.ua
сторінка курсу в Classroom - https://classroom.google.com/c/NzIzNjQyNjIyMTQ3?cjc=h36vpp4
код доступу - h36vpp4</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="3">12 Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="2">доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="3">125 Кібербезпека та захист інформації</td><td>Семестр</td><td colspan="2">1, 2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="3">Кібербезпека</td><td>Тип дисципліни</td><td colspan="2">Цикл обов’язкових компонент ОНП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>4</td><td>120</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
36</td><td>Лабораторних занять
-</td><td>Самостійна підготовка
66</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Патентознавство та авторське право.
Англійська мова наукового спрямування.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Теоретичні та практичні проблеми технічного захисту інформації.
Сучасні методи управління інформаційною та кібербезпекою.</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь застосування методів дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з створенням методів і засобів забезпечення кібербезпеки на основі сучасних математичних методів, інформаційних технологій.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Фахові компетентності (СК)</td></tr>
<tr><td colspan="4"></td><td colspan="5">ФК-3. Організаційно-комунікативна компетентність (у специфічних сферах управлінської діяльності) – здатність до лідерства та новаторської діяльності, до формування високого рівня комунікативної культури; здатність переконувати оточуючих, стверджувати свою позицію; володіння державною мовою, грамотним усним та писемним діловим мовленням, ораторським мистецтвом, професійним етикетом, а також навичками публічної презентації результатів роботи, вміннями обирати відповідні форми і методи презентації; володіння іноземними мовами, уміння правильно розмовляти та писати різними комунікативними стилями, а саме неофіційним, офіційним та науковим тощо.
ФК-4. Професійна компетентність – стан теоретичної та практичної підготовленості, що забезпечує ефективність вирішення професійних проблем і типових професійних завдань; стан володіння інформаційними технологіями та технологіями захисту інформації; здатність до удосконалення та впровадження у практику інновацій у сфері інформаційної та кібербезпеки; ступінь використання наукової літератури та інших джерел інформації для реалізації інноваційних</td></tr>
</table>

	технологій; здатність до здійснення ефективного пошуку та структурування інформації, до кваліфікованої роботи з різними IP тощо. **ФК-5. Загальнонаукова компетентність** – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо. **ФК-6. Політехнічна компетентність** – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування 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.
Програмні результати навчання (ПРН)	
ПРН-14. Володіти навиками роботи із спеціалізованими системами криптохзахисту та криптоаналізу, управляти змінами при роботі з існуючими системами криптографічного захисту. **ПРН-18. Уміти** аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів. **ПРН-19. Уміти** проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці. **ПРН-20. Уміти** визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів. **ПРН-22. Уміти** розробляти та впроваджувати дослідницькі проекти в галузі знань «Інформаційні технології» спеціальності «Кібербезпека та захист інформації» для забезпечення безпеки мережевої інфраструктури. **ПРН-23. Бути здатним** генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки.	

ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.
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. Методологія реалізації систем виявлення вторгнень			
Тема 1. Класифікація атак та механізми їх реалізації в інформаційній системі **Знати**: класифікацію, основні визначення та механізми реалізації атак в інформаційних системах. **Вміти:** застосовувати основні етапи збору інформації та механізми для реалізації атак. **Формування компетентностей:** ФК-5, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН30. **Рекомендовані джерела:** 1-4, 8-16	Лекція 1. 2 години		Лекція-візуалізація
	Практичне заняття 1 4 години	5 балів	Створення моделі атак на основі основних механізмів реалізації атаки: вивчення навколишнього середовища, ідентифікації топології мережі, ідентифікації вузлів, ідентифікації сервісів, сканування портів, визначення ролі вузла в інформаційній системі. Види реалізації атаки: проникнення, встановлення контролю, визначення мети атаки. Етапи завершення атаки.
Тема 2. Теоретичні основи побудови системи виявлення вторгнень (СВВ) **Знати**: основні компоненти багаторівневого захисту інформаційних систем, класифікувати СВВ за принципом реалізації. **Вміти**: застосовувати статистичні та динамічні СВВ. **Формування компетентностей:** ФК-4, ФК-6. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН27. **Рекомендовані джерела:** 1-4, 8-16	Лекція 2. 2 години		Лекція-візуалізація.
	Практичне заняття 2. 4 години	5 балів	Вивчення основних методів та засобів побудови СВВ, їх призначення, функції та місце в інформаційній системі.
Тема 1. Класифікація атак та механізми їх реалізації в інформаційній системі. **Тема 2.** Теоретичні основи побудови системи виявлення вторгнень.	Самостійна робота 14 годин	3 бали	1. Етапи реалізації атак. 2. Проблема визначення аномалій в інформаційних системах організацій.
Розділ 2. Методи аналізу виявлення аномалій мережевого трафіку			
Тема 3. Технології функціонування систем виявлення атак **Знати**: технології виявлення аномальної активності, сигнатурні методи, виявлення аномалій на основі протоколів. **Вміти**: користуватись базами виявлення аномалій. **Формування компетентностей:** ФК-4, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН26. **Рекомендовані джерела:** 1, 4, 6-9	Лекція 3. 2 години		Лекція-візуалізація.
	Практичне заняття 3. 4 години	5 балів	Вивчення основних баз виявлення аномальних даних в інформаційній системі. Методи виявлення вторгнень Bro, OSSEC, STAT, Prelude, Snort, SnortNet, AAFID.

Тема 4**. Технології аналізу мережевого трафіка.** **Знати**: Програми аналізу та моніторингу мережевого трафіку, програми-аналізатори мережевого трафіку, алгоритм проведення аналізу. **Вміти**: застосовувати програми аналізатори мережевого трафіку **Формування компетентностей:** ФК-4, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН26. **Рекомендовані джерела:** 1, 4, 6-9	Лекція 4. 2 години		Лекція-візуалізація.
	Практичне заняття 4. 4 години	5 балів	Установка, налаштування програм аналізаторів трафіка: система моніторингу Cacti, DUTrffic Bandwidth Monitor Pro, Wireshark.
Тема 4. Технології аналізу мережевого трафіка. **Тема 3.** Технології побудови систем виявлення атак.	Самостійна робота 14 годин	3 бали	1. Концепції виявлення загроз. 2. Програми аналізу та моніторингу трафіка.
Розділ 3. Методи виявлення аномалій в інформаційних системах			
Тема 5. Методи виявлення аномальної поведінки процесів функціонування інформаційних систем. **Знати**: основні методи виявлення невідомих атак та вторгнень, формувати образ нормального функціонування інформаційної системи, оптимальний набір для параметрів оцінки, визначати показник аномальності. **Вміти**: визначати основні показники нормального функціонування інформаційної системи. Проводити оцінку ефективності алгоритмів виявлення аномальної поведінки. **Формування компетентностей:** ФК-4, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН26. **Рекомендовані джерела:** 1, 2, 3, 6, 12-13	Лекція 5. 2 години		Лекція-візуалізація.
	Практичне заняття 5. 4 години	5 балів	Модель нормального функціонування ІС, визначення параметрів оцінки, показники аномальності.
Тема 6. Виявлення аномальних викидів трафіку методами кратномаштабного аналізу **Знати**: знати основи теорії вейвлетов, непреривне та дискретне вейвлет перетворення **Вміти**: виконувати згортку, застосовувати швидке вейвлет перетворення. **Формування компетентностей:** ФК-4, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН26. **Рекомендовані джерела:** 8-15	Лекція 6. 2 години		Лекція-візуалізація.
	Практичне заняття 6. 4 години	5 балів	Моделювання вейвлет перетворювань.
Тема 7. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу **Знати**: напрями використання методів фрактального аналізу **Вміти**: здійснювати виявлення DoS- і DdoS-атак **Формування компетентностей:** ФК-4, ФК-6, ФК-7. **Результати навчання:** ПРН18, ПРН19, ПРН20, ПРН26. **Рекомендовані джерела:** 4, 12-13	Лекція 7. 2 години		Лекція-візуалізація.
	Практичне заняття 7. 4 години	5 балів	Проводити моделювання DoS- і DdoS-атак.

Тема 5. Методи виявлення аномальної поведінки процесів функціонування інформаційних систем. **Тема 6.** Виявлення аномальних викидів трафіку методами кратномаштабного аналізу **Тема 7.** Виявлення DoS- і DdoS-атак методами мультифрактального аналізу.	Самостійна робота 24 години	5 балів	1. Міжнародний стандарт NIST 800-31 2. Дискретне вейвлет-пакетне перетворення. 3. Виявлення DoS- и DdoS-атак методами мультифрактального аналізу.
Розділ 4. Перспективні методи досліджень у сфері кібербезпеки			
Тема 8. Методологія побудови інтелектуальних систем захисту. **Знати**: системні принципи захисту інформації, функції безпеки,поняття функції інтелектуалізації захисту, структуру інтелектуальної машини, нейромережеві системи виявлення атак. **Вміти**: використовувати нейромережеві системи виявлення атак, алгоритми штучних імунних систем. **Формування компетентностей:** ФК-3, ФК-5. **Результати навчання:** ПРН14, ПРН22, ПРН23, ПРН27, ПРН30. **Рекомендовані джерела:** 2,3, 6-17	Лекція 8. 2 години		Лекція-візуалізація, експрес-опитування здобувачів
	Практичне заняття 8. 4 години	5 балів	Моделювання інтелектуальних систем захисту.
Тема 9. Штучний інтелект в системах захисту інформації **Знати**: роль та місце штучного інтелекту в системах захисту інформації, механізми функціонування. **Вміти**: застосовувати методи виявлення аномалій на основі механізмів штучного інтелекту. **Формування компетентностей:** ФК-3, ФК-5. **Результати навчання:** ПРН14, ПРН22, ПРН23, ПРН27, ПРН30. **Рекомендовані джерела:** 2, 3, 8-17	Лекція 9. 2 години		Лекція-візуалізація, експрес-опитування здобувачів.
	Практичне заняття 9. 2 години	5 балів	Когнітивне моделювання.
Тема 8. Методологія побудови інтелектуальних систем захисту. **Тема 9.** Штучний інтелект в системах захисту інформації.	Самостійна робота. 14 годин	4 бали	1. Нейромережеві системи виявлення атак. 2. Практичне застосування штучного інтелекту в системах виявлення аномалій.
Іспит	Практичне заняття 10. 2 години	40 балів	Іспит у письмовій формі.
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Комп’ютерне обладнання, мережа Інтернет, програмні комплекси Nessus Professional, Tenable.sc, IBM QRadar SIEM та ESET Protect.			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
1. NIST SPECIAL PUBLICATION 800-94 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf 2. Artificial Intelligence in Cyber Security: Theories and Applications. Springer Cham. 978-3-031-28581-3 Published: 06 October 2023. https://link.springer.com/book/10.1007/978-3-031-28581-3#bibliographic-information . https://doi.org/10.1007/978-3-031-28581-3 . 3. Fei Hu, Xiali Hei AI, Machine Learning and Deep Learning. A Security Perspective/ ISBN 9781032034058 346 Pages 136 B/W Illustrations December 19, 2024 by CRC Press. 4. N. N. R. Ranga Suri Athithan Outlier Detection: Techniques and Application./ N. N. R. Ranga Suri, Narasimha Murty M, G. - Springer Nature Switzerland. 2019. 227p. 5. Борсуковський Ю.В., Борсуковська В.Ю., Гайдур Г.І., Складанний П.М., Бурячок В.Л., Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку: навчальний посібник / ISBN 978-617-574-272-3 / УДК 32.973я73 р. / – Львів - Видавництво «Магнолія 2006», 2023, 222 с.			

6. Гайдур Г.І., Гахов С.О. Теоретичний підхід до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи. Телекомунікаційні та інформаційні технології. 2021. № 1 (70). С. 79-87. https://doi.org/10.31673/2412-4338.2021.017987
7. Гахов С. О. Застосування положень імунології в теорії захищених інформаційних систем. Сучасний захист інформації. 2018. № 2. С. 59 – 64. https://journals.dut.edu.ua/index.php/dataprotect/article/view/1902/1805 .
8. Гайдур Г. І., Шулімова Д. Д., Бойко А. О., Постніков Є. І. Модель забезпечення кібербезпеки інтернету речей. Телекомунікаційні та інформаційні технології. № 2 (2024). С 4-13. https://doi.org/10.31673/2412-4338.2024.020515
9. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003
10. Гайдур,Г. І., & Бригинець,А. А. (2024). Захист конфіденційних даних у снепшотах Amazon Elastic Block Store. Сучасний захист інформації, 1(57), 15–21. https://doi.org/10.31673/2409-7292.2024.010002 .
11. Легомінова, С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. – 2023. - №2(22). – С. 564-67. https://doi.org/10.28925/2663-4023.2023.22.5467
12. Гайдур Г. І., Гахов С. О., Бригинець А. А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. https://doi.org/10.31673/2412-4338.2023.016173
13. Гайдур Г. І. Гахов С. О, Сич М. В., Дмітрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. https://doi.org/10.31673/2412-4338.2023.031221
14. Haidur, H. The Method of Increasing the Efficiency of Signal Processing Due to the Use of Harmonic Operators // Zamrii, I., Haidur, H., Sobchuk, A., Zinchenko, K., Polovinkin, I. // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 138–141. https://doi.org/10.1109/atit58178.2022.10024212 (Scopus).
15. Гайдур Г.І., Гахов С.О., Марченко В.В. Метод побудови динамічної моделі логічного об'єкта інформаційної системи та визначення закону його функціонування. Radioelectronic and Computer Systems, 2022, no. 1(101). С. 129-140. https://doi.org/10.32620/reks.2022.1.10 . (Категорія А, Scopus).
16. Soni, P. IDS/IPS : An In-Depth Guide to IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Defending the Digital Fortress. . URL^ https://www.amazon.in/IDS-IPS-Depth-Intrusion-Prevention-ebook/dp/B0CDHF1GTW
17. Вступ до квантової криптології [Текст]: Навчальний посібник (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, В.К. Задірака, О.М. Хіміч, Ю.І. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко.]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2023. – 691 с.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і семінарських занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

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

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	45 балів
	• Самостійна робота	15 балів

ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі..	40 балів

Додаткова оцінка	
Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції.	3 бали
- Стаття у фаховому виданні.	5 балів
- Стаття в іноземному рецензованому виданні.	10 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.	

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в заліковій відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних/контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни.	Добре / Зараховано (В)
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість	Добре / Зараховано (С)

	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.	використання теоретичних положень для практичного використання викликають утруднення.	
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

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