Затверджено
завідувач кафедри
СТКБ_____ Г. Гайдур
«31» 08 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«НАУКОВА КОМУНІКАЦІЯ ТА ТЕХНІЧНИЙ ПЕРЕКЛАД В КІБЕРБЕЗПЕЦІ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Гайдур Галина Іванівна, доктор технічних наук, професор</td><td>Контактна інформація лектора (e-mail), сторінка курсу</td><td colspan="3">e-mail: g.haidur@duikt.edu.ua
https://classroom.google.com/c/ODY4MDEwMDU3ODk0</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">F Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="3">другий (магістерський) рівень</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">F5 Кібербезпека та захист інформації</td><td>Семестр</td><td colspan="3">1, 2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Освітньо-професійна програма «Інформаційна та кібернетична безпека»</td><td>Тип дисципліни</td><td colspan="3">Обов’язкова компонента освітньо-професійної програми</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>6</td><td>180</td><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td colspan="3"></td><td></td><td>-</td><td>36
36</td><td>-</td><td>54
54</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Прикладна загальна теорія систем інформаційної та кібербезпеки, Технології виявлення уразливостей мережевих ресурсів</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Науково-дослідна практика</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки., принципи академічного письма та коректного цитування.</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 / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.</td><td colspan="5">КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.</td></tr>
</table>

КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ6, КФ7, КФ8, КФ9, КФ10	КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Програмні результати навчання (ПРН)	
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	

РН20. Ставити та вирішувати складні інженерно прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Практика перекладу наукових та технічних текстів <u>Знати</u>: особливості та загальні підходи до технічного перекладу, види та переклад технічної літератури. Оформлення джерел. ***<u>Формування компетенцій:</u>*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***<u>Програмні результати навчання:</u>*** РН1, РН2, РН17, РН20, РН23. ***<u>Рекомендовані джерела:</u>*** 1-4.	Практичне заняття 1 2 год	4	Практичні підходи до технічного перекладу.
Тема 2. Типологія наукової інформації та основні види видань ***<u>Знати:</u>*** термін наукова інформація, первинні і вторинні документи, періодичні, неперіодичні видання. ***<u>Формування компетенцій:</u>*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***<u>Програмні результати навчання:</u>*** РН1, РН2, РН17, РН20, РН23. ***<u>Рекомендовані джерела:</u>*** 1-4.	Практичне заняття 2 2 год	4	Обговорення типів наукової інформації
Тема 3. Наукометричні бази. ***<u>Вміти:</u>*** класифікацію і види наукометричної бази (Україна та міжнародна.. Web of Science, Scopus, Google Scholar, Index Copernicus, ***<u>Формування компетенцій:</u>*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***<u>Програмні результати навчання:</u>*** РН1, РН2, РН17, РН20, РН23. ***<u>Рекомендовані джерела:</u>*** 1-4.	Практичне заняття 3-5 6 год	4	Дискусія

Тема 4 **Інформаційно-аналітична діяльність фахівців з кібербезпеки для розв'язування складних задач кібербезпеки.** ***Знати***: знати застосовувати бази знань з вирішення питань кібербезпеки відповідно до сучасних практик та стандартів кібербезпеки. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 6 2 год	6	Практичне вирішення задач з пошуку наково-технічних текстів в сфері кібербезпеки
Тема 5. Науково-технічний переклад: «Cybersecurity Introduction and Overview». ***Introduction to Cybersecurity*** ***Difference Between Information Security and Cybersecurity*** ***Cybersecurity Objectives*** ***Cybersecurity Governance*** ***Cybersecurity Domains*** ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 7-9 6 год	6	Практична робота перекладу наукових текстів з кібербезпеки
Тема 6. Науково-технічний переклад: Cybersecurity Concepts ***Risk*** ***Risk Standards*** ***Common Attack Types and Vectors*** ***Common Attack Types and Vectors*** ***Policies*** ***Cybersecurity Controls*** ***Знати***: ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 10-12 6 год	6	Практична робота перекладу наукових текстів з кібербезпеки

Тема 7. Науково-технічний переклад: Security Architecture Principles ***Overview of Security Architecture*** ***The OSI Model*** ***Defense in Depth*** ***Information Flow Control*** ***Isolation and Segmentation*** ***Logging, Monitoring and Detection*** ***Encryption Fundamentals, Techniques and Applications*** ***Знати***: ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 13-17 10 год	6	Практична робота перекладу наукових текстів з кібербезпеки
Тема 8. Формування звітів у мультидисциплінарних контекстах. Залік. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 18 2 год	6	Практична робота перекладу наукових текстів з кібербезпеки
Застосування світових практик, стандартів у професійній діяльності в сфері кібербезпеки, щодо вирішення складних інженерно прикладних та наукових задач кібербезпеки. Підготовка статей, участь у конференціях	Самостійна робота 54 год	18	Доповіді на конференціях, практичний досвід написання статей.
Частина 2			
Тема 9. Редактор LaTeX для роботи з науково-технічними текстами ***Вміти:*** застосовувати та редагувати науково-технічні тексти з використанням сучасних технологій ***Формування компетенцій:*** КЗ1, КЗ2, КЗ4, КЗ5, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-5.	Практичне заняття 1-6 12 год	15	Практична робота з створення наукових текстів з кібербезпеки
Тема 10. Науково-технічний переклад: Incident Response ***Event vs. Incident***	Практичне заняття 7-10	5	Практична робота перекладу наукових текстів з кібербезпеки

Security Incident Response ***Investigations,*** ***Legal Holds and Preservation*** ***Forensics*** ***Disaster Recovery and Business Continuity Plans*** ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач., мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	10 год		
Тема 11. Науково-технічний переклад: Security of Network Syst Apps Data ***Process Controls. Risk Assessments*** ***Process Controls. Vulnerability Management*** ***Process Controls. Penetration Testing*** ***Network Security*** ***Operating System Security*** ***Application Security*** ***Data Security*** ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 11-14 8 год	10	Практична робота перекладу наукових текстів з кібербезпеки
Тема 12. Науково-технічний переклад: Privilege Cybersecurity Getting started with zero trust Classifying users Enforcing least privilege Meeting compliance Defining Least Privilege Cybersecurity ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері кібербезпеки. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3.	Практичне заняття 15-16 4 год	5	Практична робота перекладу наукових текстів з кібербезпеки

Програмні результати навчання: РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.			
Тема 13. Науково-технічний переклад: The Importance and Role of the SOC ***Вміти:*** інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач, мати навички автономного і самостійного навчання у сфері. ***Формування компетенцій:*** К31, К32, К34, К35, КФ3. ***Програмні результати навчання:*** РН1, РН2, РН17, РН20, РН23. ***Рекомендовані джерела:*** 1-4.	Практичне заняття 17-18 4 год	5	Практична робота перекладу наукових текстів з кібербезпеки
Застосування світових практик, стандартів у професійній діяльності в сфері кібербезпеки, щодо вирішення складних інженерно прикладних та наукових задач кібербезпеки. Підготовка статей, участь у конференціях	Самостійна робота 54 год	20	Доповіді на конференціях, практичний досвід написання статей.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Mary Manjikian Cybersecurity Ethics: An Introduction. *Routledge.* 2022. p 282.11 Strategies of a World-Class Cybersecurity Operations Center. *The MITRE Corporation*. ALL RIGHTS RESERVED. 2022. p 452.
2. Scopuc URL: https://www.elsevier.com/solutions/scopus
3. Web of Science URL: https://www.webofscience.com/wos/woscc/basic-search
4. База знань Overleaf URL: https://www.overleaf.com/learn .
5. 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. DOI: 10.31673/2412-4338.2024.020515
6. 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
7. 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.
8. Скибун,О. Ж., Гайдур,Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006 .
9. 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. DOI 10.28925/2663-4023.2023.22.5467
10. Ганченко М.І., Гайдур Г.І., Гахов С.О., Дмітрієв В.Є. "Актуальність та перспектива розвитку Privileged Access Management рішень." Зв'язок. 2022. №1 (2022). С. 3-9. DOI: 10.31673/2412-9070.2022.010310 Доступ: https://con.dut.edu.ua/index.php/communication/article/view/2578
11. 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. DOI: 10.31673/2412-4338.2023.016173

12. 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. DOI: 10.31673/2412-4338.2023.031221
13. 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.(Scopus)
14. 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. doi: 10.32620/reks.2022.1.10. (Категорія А, Scopus).

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.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 30-60 балів у сукупності за всіма темами дисципліни (залік)
Умовою допуску до підсумкового контролю є набрання студентом 30-60 балів у сукупності за всіма темами дисципліни (екзамен))

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	42 / 40 балів
	• Самостійна робота	18 / 20 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10-15 балів за рішенням викладача
ПІДСУМКОВЕ ОЦІНЮВАННЯ *Залік* *Екзамен*	Метою заліку (екзамену) є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій або усній формі. Екзамен проходить у письмовій або усній формі.	40 балів 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	**Високий** Повністю забезпечує вимоги до знань,	Відмінно / Зараховано (А)

	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.	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.	
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)
67-74	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)
60-66	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.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання)

	Цілісність розуміння матеріалу з дисципліни у студента відсутні.		/ Не зараховано (FX) *В залікову книжку не проставляється*
0-34	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*

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.