СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«АВТОМАТИЗАЦІЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ »

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Іванченко Ігор Сергійович,
кандидат технічних наук, доцент,
професор кафедри технічних систем кіберзахисту</td><td>Контактна інформаціялектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: i.ivanchenko@duikt.edu.ua

сторінка курсу в Classroom:
https://classroom.google.com/c/NzExNzY2NDAxMTUy?cjc=oam5tv2

код доступу: oam5tv2</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">F «Інформаційні технології»</td><td>Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">F5 Кібербезпека та захист інформації</td><td>Семестр</td><td colspan="2">1</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Технічні системи інформаційного та кібернетичного захисту</td><td>Тип дисципліни</td><td colspan="2">Цикл вибіркових компонент ОПП</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
24</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
12</td><td>Самостійна підготовка
96</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">Опанування студентами необхідних теоретичних знань із створення електронних документів та електронного документообігу інформації з обмеженим доступом, побудови автоматизованих та інформаційних систем обробки інформації та управління, сучасних методів та засобів захисту інформації з обмеженим доступом. Надання практичних навиків із створення електронних документів та електронного документообігу, захисту інформації з обмеженим доступом в автоматизованих та інформаційних системах.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (КЗ)</td><td colspan="4">Hard-skills / Фахові компетентності (КФ)</td></tr>
</table>

КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ7. Вміння виявляти, ставити та вирішувати проблеми. КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ10. Здатність застосовувати кращі практики у професійній діяльності.	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. 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 та стандарти у професійній діяльності у 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. 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 оцінювати ефективність їх використання. КФ12. Здатність розробляти технічну документацію для проведення тестування, налагоджування та допоміжних заходів щодо функціонування та експлуатації систем захисту інформації на об’єктах інформаційної діяльності.

Програмні результати навчання (РН)	
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати інформаційні технології, фізичні та математичні моделі у сфері інформаційної безпеки та/або кібербезпеки. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти і практики з метою розв’язання складних задач професійної діяльності у сфері інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. РН10. Забезпечувати безперервність бізнес/операційних процесів, виявляти уразливості інформаційних систем і ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегій і політик інформаційної безпеки та/або кібербезпеки організації. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи і засоби криптографічного та технічного захисту інформації, а також аналізувати і надавати оцінку ефективності їх використання.	

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних і світових стандартів та кращих практик. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, необхідних для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 «Правове забезпечення та автоматизовані системи обробки інформації з обмеженим доступом» »			
Тема 1. ***Вступ до дисципліни. Автоматизація обробки інформації з обмеженим доступом. Поняття інформації та її види. Способи та режими автоматизованої обробки інформації.*** ***Знати***: правові основи захисту інформації та інформаційної безпеки. Основні напрямки розвитку науки й техніки в області захисту інформації та інформаційної безпеки. Сучасні методи та системи захисту інформації з обмеженим доступом під час її автоматизованої обробки. закон України про захист інформації в інформаційно-телекомунікаційних системах, перелік відомостей, що становлять службову інформацію і яким присвоюється гриф з обмеженим доступом «для службового користування», кількісну оцінку стійкості парольного захисту, використання цифрового підпису і шифрування електронних повідомлень, злочини проти конфіденційності, цілісності і доступності комп'ютерних даних та систем, злочини, пов'язані з використанням комп'ютерів, злочини, пов'язані з порушенням авторських і суміжних прав з використанням комп'ютерних даних і систем, злочин, пов'язані зі змістом даних.	Лекція 1 **2 години**	**5*3=15 балів**	Лекція-візуалізація
	Практичне заняття 1 **2 години**		Усне опитування, навчальна дискусія,обговорення ситуаційного завдання
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 2 **2 години**		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Лабораторне заняття 1 **2 години**		Комп'ютерна аудиторія. 2 Кількісна оцінка стійкості парольного захисту
	Лабораторне заняття 2 **2 години**		Комп'ютерна аудиторія. Використання цифрового підпису і шифрування електронних повідомлень
	Лекція 3 **2 години**		Лекція-візуалізація

	Практичне заняття 3 **2 години**		Проведення модульного контролю
	Лекція 4 **2 години**		Лекція-візуалізація, експрес-опитування студентів

Вміти: Уміти обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів. Формування компетентностей: К31, К33, К39, К310; КФ2, КФ8. Результати навчання: РН4, РН7, РН13, РН20. ***Рекомендовані джерела:*** 1, 3–10,14-20	Лекція 5 **2 години**		Лекція-візуалізація, експрес-опитування студентів
Тема 2. ***Загальна характеристика інформаційних систем. Класифікація інформаційних систем обробки інформації.*** ***Знати***: принципи побудови автоматизованих та інформаційних систем обробки інформації та управління, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації, типове положення про службу захисту інформації в автоматизованій системі, сканування мереж, захист від копіювання. прив'язку до апаратного забезпечення. використання реєстру, ***Вміти***: уміти обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності,, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. Формування компетентностей: К31, К33, К34, К37; КФ1, КФ3, КФ8. Результати навчання: РН4, РН6, РН8, РН13, РН23. ***Рекомендовані джерела:*** 2–10,14-20	Лекція 6 **2 години**	**5*3=15 балів**	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 4 **2 години**		Усне опитування, навчальна дискусія,обговорення ситуаційного завдання
	Лабораторне заняття 3 **2 години**		Комп'ютерна аудиторія. Сканування мереж.
	Лабораторне заняття 4 **2 години**		Комп'ютерна аудиторія. Захист від копіювання. Прив'язка до апаратного забезпечення. Використання реєстру
	Практичне заняття 5 **2 години**		Усне опитування, навчальна дискусія,обговорення ситуаційного завдання
	Лекція 7 **2 години**		Лекція-візуалізація, експрес-опитування студентів

	Лекція 8 **2 години**		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 6 **2 години**		Проведення модульного контролю
Розділ 2 «ОРГАНІЗАЦІЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ОБМЕЖЕНИМ ДОСТУПОМ»			
Тема 3. ***Розвиток автоматизованих систем обробки інформації та їх конвергенція з телекомунікаційними мережами*** ***Знати***: порядок створення електронних документів з обмеженим доступом. ***Вміти***: використовувати спеціалізовані програмні пакети, протоколи передачі даних, спеціальну мікропроцесорну техніку, володіти сучасними інформаційними та безпековими технологіями,	Лекція 9 **2 години**		Лекція-візуалізація, експрес-опитування студентів
	Лекція 10 **2 години**		Лекція-візуалізація, експрес-опитування студентів
	Лабораторне заняття 5 **2 години**	**3*2=6 балів**	Комп'ютерна аудиторія. Захист інформації при застосуванні особистої системи мережевого захисту Comodo Firewall
	Практичне заняття 7 **2 години**		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
Тема 4. ***Загальні принципи побудови автоматизованих систем обробки інформації*** ***Знати***: порядок функціонування електронного документообігу, організаційні заходи та технічні засоби захисту інформації з обмеженим доступом під час її автоматизованої обробки. ***Вміти:*** підтримувати комплексні системи інформаційного захисту в стані, необхідному для вирішення завдань захисту інформації. Формувати документальні матеріали, заповнювати документи. Складати плани для швидкого відновлення виробничих процесів у випадку серйозних перебоїв у роботі підрозділів. Створювати службові електронні документи. Аналізувати можливі загрози безпеки інформаційної системи. Визначати модель порушника в інформаційній системі. Аналізувати захищеність обробленої інформації в інформаційних системах на випадок несанкціонованого доступу. Визначати вимоги захисту інформації в комп`ютерних системах на випадок несанкціонованого доступу. Створювати функціональні профілі захищеності інформаційної системи.	Практичне заняття 8 **2 години**	**3*3=9 балів**	Тестування, навчальна дискусія,вирішення практичних задач
	Лекція 11 **2 години**		Лекція-візуалізація, експрес-опитування студентів
	Лабораторне заняття 6 **2 години**		Комп'ютерна аудиторія. Створення службових електронних документів

Формування компетенцій:ЗК1, ЗК2, СК1 ***Результати навчання:***ПРН7, ПРН12, ПП8-ПП10, ПП18, ПП26 ***Рекомендовані джерела:*** 1–21	Лекція 12 **2 години**		Підбиття підсумків по курсу. Заключна лекція
	Практичне заняття 9 **2 години**		Проведення заліку з дисципліни
	Самостійна робота **96 годин**	**15 балів**	1. Поняття інформації зобмеженим доступом, порядок доступудо інформації з обмеженимдоступомтаспособиїїобробки. 2. Порядок створення, обробки, зберігання та пересилання електронних документівзобмеженимдоступом. 3. Принципи функціонування системи управління інформацією MS Outlook, структура та принципи побудови крипто протоколів захищеного обміну данимиSFTP,SSH,HTPS,SSLv3,TLS. 4. Організаційні заходи та технічні засоби захисту інформації з обмеженим доступомвавтоматизованихтаінформаційнихсистемахобробкиінформації. 5. Порядокстиснення даних та криптографічні перетворення інформації для її захисту. 6. Призначення та структура DLP систем запобігання витоку інформації з обмеженимдоступом. 7. Порядок розробки плану захисту інформації з обмеженим доступом для створенняКСЗІвІТС

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ
• Мультимедійний проектор; • Комп’ютерний клас для проведення лабораторних та практичних занять. • Програмне забезпечення. Windows XP, 8,10, Microsoft Office, Ultra Zip Password Cracker 1.00 та Advanced ZIP Password Recovery 2.2, Network Skanner, Kasperski, Total Security, Chrome, IE, Mozilla Firefox, Opera, Acronis Disk Director, SimPass.
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2019.-276с
2. Голубенко О.Л. Політика інформаційної безпеки / О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ: Вид: СНІ ім. В.Даля, 2019. – 300 с.
3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2019. – 608 с.
4. Департамент спеціальних телекомунікаційних систем та захисту інформації служби безпеки України. Н а к а з N 53 від 30.11.99. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації.
5. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
6. Закон України. Про державну таємницю. (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93)
7. Закон України. Про електронні документи та електронний документообіг. (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275).
8. Закон України. Про захист інформації в автоматизованих системах. (Відомості Верховної Ради (ВВР), 1994, N 31, ст.286).
9. Закон України. Про захист інформації в інформаційно-телекомунікаційних системах. Закон введено в дію з дня опублікування - 2 серпня 1994 року (згідно з Постановою Верховної Ради України.
10. Закон України. Про Національну систему конфіденційного зв'язку. (Відомості Верховної Ради України (ВВР), 2002, № 15, ст.103).
11. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л.: монографія “Базова модель експертної системи оцінки безпеки інформації в комп‘ютерних системах органів внутрішніх справ України” (шифр “Торсіон-1”). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту “Торсіон-1”. – К.: Видавництво НАВСУ, 2003. – 316с.
12. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2018. – 223 с
13. Наказ від 04.07.2008 N 112. Адміністрація державної служби спеціального зв'язку та захисту інформації України. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
14. НД ТЗІ 3.7-003 -2005 СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. Затверджено наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 8 листопада 2005 р. № 125. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
15. Перелік відомостей, що становлять службову інформацію і яким присвоюється гриф «Для службового користування» Затверджено 03.09.2022. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України.
16. Постанова Кабінет міністрів України від 29 березня 2006 р. N 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
17. Стандарт ISO/1EC 15408:2000. Information technology − Security techniques -Evaluation criteria for IT security.
18. Стандарт ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.
19. Указ президента України №56/2022. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»
20. Шорошев В.В. Основи формування політики безпеки комп’ютерних систем: наукове видання. – К.: Бізнес і безпека, 2016. – 141с.

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.

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, проведення тестових розрахунків рівнів сигналів для їх подальшого аналізу, поглиблене вивчення матеріалу 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 консультується з викладачем.
- 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	**27 балів**
	• Виконання лабораторних робіт	**18 балів**
	• Самостійна робота	**15 балів**
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою *заліку* є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків.	40 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- тези доповіді на фаховій конференції;	2 бали
- стаття у фаховому виданні України;	6 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 (A)
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 (B)
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 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	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.