СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«СТАНДАРТИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Поночовний Петро Михайлович, PhD? доцент кафедри Технічних систем кіберзахисту</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: p.ponochovnyi@duikt.edu.ua
сторінка курсу в Classroom:
https://classroom.google.com/c/ODc2ODk1NTU0ODI5?cjc=bsjc4kup
код доступу – bsjc4kup</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Другий магістерський</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">125 Кібербезпека та захист інформації</td><td colspan="2">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 colspan="2">Тип дисципліни</td><td colspan="2">Обов'язкова компонента ОПП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій
24</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
18</td><td colspan="2">Самостійна підготовка
30</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 для яких є базовою</td><td colspan="6">Ліцензування , атестація та сертифікація у сфері безпеки ОІД, Організація і проведення спеціальних досліджень на ОІД, Кваліфікаційна робота</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">формування у здобувачів вищої освіти системи теоретичних знань та практичних навичок щодо застосування, впровадження та аудиту національних і міжнародних стандартів кібербезпеки (зокрема серії ISO/IEC 27000, NIST, CIS), розробки політик управління інформаційною безпекою та забезпечення захисту конфіденційної інформації на об'єктах інформаційної діяльності.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (КЗ)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ10. Здатність застосовувати кращі практики у професійній діяльності.</td><td colspan="5">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.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою організації... з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів 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 в цілому.
КФ11. Здатність створювати методики ліцензування, атестації та сертифікації у сфері захисту інформації на об'єктах інформаційної діяльності.
КФ12. Здатність розробляти технічну документацію для проведення тестування, налагоджування та допоміжних заходів щодо функціонування та експлуатації систем захисту інформації на об'єктах інформаційної діяльності.</td></tr>
</table>

Програмні результати навчання (РН)			
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. **РН7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі 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. **РН14.** Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій бізнес операційних процесів у сфері інформаційної та/або кібербезпеки в цілому..			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1: « Еволюція міжнародних та національних стандартів інформаційної безпеки ». **Знати**: історію розвитку, структуру та призначення базових міжнародних (ISO, NIST) і національних стандартів з інформаційної безпеки **Вміти**: аналізувати та порівнювати структури різних стандартів, знаходити відповідні нормативні документи у міжнародних та національних реєстрах. **Формування компетентностей: КЗ1, КЗ3, КФ2.** **Результати навчання: РН1, РН7**. **Рекомендовані джерела:** 1,3,8.			
Історичний розвиток та класифікація стандартів інформаційної безпеки.	Лекція 1 2 год	-	Лекція-презентація.
Порівняльний аналіз структур стандартів (BS 7799, серія ISO, NIST).	Практичне заняття 1 2 год	2 бали	Отримання навичок проведення порівняльного аналізу структур міжнародних та національних стандартів інформаційної безпеки (BS 7799, серія ISO, NIST).
Робота з офіційними реєстрами стандартів та мапінг базових вимог.	Лабораторне заняття 1 2 год	4 бали	Оволодіння навичками роботи з офіційними реєстрами стандартів та здійснення мапінгу базових вимог кібербезпеки.
Вивчення термінологічної бази стандартів (ISO/IEC 27000).	Самостійна робота 1 3 год	-	Самостійна підготовка. Вивчення та аналіз термінологічної бази стандартів серії ISO/IEC 27000.
Тема 2: «Система управління інформаційною безпекою (СУІБ) за ISO/IEC 27001**».** **Знати**: архітектуру, основні процеси та вимоги стандарту ISO/IEC 27001 щодо побудови та сертифікації СУІБ. **Вміти**: розробляти Політику інформаційної безпеки та формувати «Положення про застосовність» (Statement of Applicability) для організації. **Формування компетентностей:** КЗ10, КФ4. **Результати навчання:** РН2, РН7. **Рекомендовані джерела:** 3,4,5.			
Архітектура та основні вимоги стандарту ISO/IEC 27001.	Лекція 2 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Процес впровадження та підготовка до сертифікації СУІБ в організації.	Лекція 3 2 год	-	Лекція-презентація, експрес-опитування здобувачів.

Розробка Політики інформаційної безпеки організації за вимогами ISO 27001.	Практичне заняття 2 2 год	2 бали	Отримання навичок розробки Політики інформаційної безпеки організації згідно з вимогами стандарту ISO/IEC 27001.
Розробка «Положення про застосовність» (Statement of Applicability).	Лабораторне заняття 2 2 год	4 бали	Отримання навичок формування та обґрунтування «Положення про застосовність» (Statement of Applicability) для обраної організації.
Опрацювання додатку A (Controls) стандарту ISO/IEC 27001.	Самостійна робота 2 4 год	-	Самостійна підготовка. Опрацювання вимог додатку A (Controls) стандарту ISO/IEC 27001 та їх адаптація до реальних умов підприємства.
Тема 3: « Управління ризиками інформаційної безпеки (ISO/IEC 27005 та NIST SP 800-30) ». **Знати**: методології оцінки, обробки та моніторингу ризиків інформаційної безпеки. **Вміти**: ідентифікувати, аналізувати ризики ІБ та розробляти план їх обробки (Risk Treatment Plan). **Формування компетентностей:** КЗ9, КФ4. **Результати навчання:** РН2, РН7. **Рекомендовані джерела:** 1,6.			
Методології оцінки та обробки ризиків інформаційної безпеки.	Лекція 4 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Ідентифікація та оцінка ризиків ІБ за заданим сценарієм.	Практичне заняття 3 2 год	2 бали	Отримання навичок ідентифікації, класифікації та оцінки ризиків інформаційної безпеки за заданим сценарієм.
Інструментальне моделювання ризиків та розробка плану обробки ризиків.	Лабораторне заняття 3 2 год	4 бали	Оволодіння навичками інструментального моделювання ризиків та розробки плану обробки ризиків (Risk Treatment Plan).
Аналіз та порівняння альтернативних методологій оцінки ризиків (OCTAVE, CRAMM, NIST SP 800-30).	Самостійна робота 3 3 год	-	Самостійна підготовка. Аналіз та порівняння альтернативних методологій оцінки ризиків (OCTAVE, CRAMM, NIST SP 800-30).
Тема 4: «Аудит інформаційної безпеки (ISO/IEC 27007 та 27008)» **Знати**: принципи, процедури та етапи проведення внутрішнього і зовнішнього аудиту СУІБ. **Вміти**: складати програму аудиту, проводити технічну перевірку та оформлювати звіт про невідповідності. **Формування компетентностей:** КЗ3, КФ9. **Результати навчання:** РН7, РН14. **Рекомендовані джерела:** 1,4,5.			
Принципи та етапи проведення аудиту СУІБ.	Лекція 5 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Технічний аудит та методика оцінки заходів безпеки.	Лекція 6 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Складання програми та плану внутрішнього аудиту СУІБ.	Практичне заняття 4 2 год	2 бали	Отримання навичок складання програми, плану та аудиторських чек-листів для проведення внутрішнього аудиту СУІБ.
Проведення імітаційного аудиту ІТС та оформлення звіту про невідповідності.	Лабораторне заняття 4 2 год	4 бали	Оволодіння навичками проведення імітаційного технічного аудиту ІТС та оформлення звіту про виявлені невідповідності.

Підготовка до проведення аудиторських інтерв'ю та аналізу свідоцтв аудиту.	Самостійна робота 4 4 год	-	Самостійна підготовка. Підготовка до проведення аудиторських інтерв'ю та збору об'єктивних аудиторських доказів.
Тема 5: «Національні стандарти України (НД ТЗІ) та захист конфіденційної інформації ». **Знати**: систему нормативних документів з технічного захисту інформації (НД ТЗІ) в Україні та вимоги до створення КСЗІ. **Вміти**: аналізувати вітчизняні нормативні документи та складати профіль захисту для автоматизованої системи. **Формування компетентностей:** К31, КФ11, КФ12. **Результати навчання:** РН8. **Рекомендовані джерела: 2,**9,12.			
Система технічного захисту інформації в Україні та створення КСЗІ.	Лекція 7 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Порівняльний аналіз вимог НД ТЗІ 2.5-004-99 та міжнародних аналогів.	Практичне заняття 5 2 год	2 бали	Отримання навичок проведення порівняльного аналізу вимог вітчизняних нормативних документів (НД ТЗІ 2.5-004-99) та їх міжнародних аналогів.
Складання профілю захисту для автоматизованої системи згідно з НД ТЗІ.	Лабораторне заняття 5 2 год	4 бали	Отримання навичок складання профілю захисту для автоматизованої системи згідно з вимогами системи НД ТЗІ.
Поглиблене вивчення нормативних документів серії НД ТЗІ.	Самостійна робота 5 3 год	-	Самостійна підготовка. Поглиблене вивчення та опрацювання нормативних документів серії НД ТЗІ щодо створення КСЗІ.
Тема 6: «Технічні критерії оцінки безпеки ІТ (Common Criteria - ISO/IEC 15408) ». **Знати**: концепцію, структуру та рівні гарантій оцінки (EAL) за стандартом Common Criteria. **Вміти**: визначати вимоги до безпеки ІТ-продуктів та розробляти структуру «Завдання з безпеки» (Security Target). **Формування компетентностей:** К33, КФ2, КФ11. **Результати навчання:** РН7, РН8. **Рекомендовані джерела:** 2,7.			
Структура, концепція та застосування стандарту Common Criteria.	Лекція 8 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Аналіз рівнів гарантій оцінки (EAL) за стандартом Common Criteria.	Практичне заняття 6 2 год	2 бали	Отримання навичок аналізу та вибору адекватних рівнів гарантій оцінки (EAL) за стандартом Common Criteria (ISO/IEC 15408).
Розробка структури «Завдання з безпеки» (Security Target) для ІТ-продукту.	Лабораторне заняття 6 2 год	4 бали	Отримання навичок розробки структури та змісту «Завдання з безпеки» (Security Target) для ІТ-продукту.
Дослідження сертифікованих засобів захисту в міжнародних реєстрах.	Самостійна робота 6 3 год	-	Самостійна підготовка. Дослідження та аналіз сертифікованих засобів захисту інформації у міжнародних реєстрах (Common Criteria Portal).
Тема 7: «Стандарти та фреймворки безпеки критичної інфраструктури (NIST CSF, CIS Controls)». **Знати**: світові підходи та фреймворки (NIST Cybersecurity Framework, CIS Controls) щодо захисту критичної інфраструктури. **Вміти**: здійснювати мапінг вимог кібербезпеки організації на NIST CSF та впроваджувати базові контролі безпеки. **Формування компетентностей:** К310, КФ4, КФ6. **Результати навчання:** РН7.			

Рекомендовані джерела: 8,11,12.			
Концепція NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).	Лекція 9 2 год	-	Лекція-презентація, експрес-опитування здобувачів.
Базові контролі кібербезпеки CIS Controls: архітектура та впровадження.	Лекція 10 2 год		Лекція-презентація, експрес-опитування здобувачів.
Мапінг вимог кібербезпеки організації на NIST Cybersecurity Framework.	Практичне заняття 7 2 год	2 бали	Отримання навичок здійснення мапінгу вимог кібербезпеки конкретної організації на структуру NIST Cybersecurity Framework.
Практична реалізація базових контролів безпеки (CIS Controls V8) у змодельованій мережі.	Лабораторне заняття 7 2 год	4 бали	Отримання навичок практичної реалізації та тестування базових контролів безпеки (CIS Controls V8) у змодельованій мережі.
Розробка профілю безпеки для об'єкта критичної інфраструктури.	Самостійна робота 7 4 год	-	Самостійна підготовка. Розробка та обґрунтування цільового профілю кібербезпеки для об'єкта критичної інфраструктури.
Тема 8: «Управління інцидентами та безперервністю бізнесу (ISO/IEC 27035, ISO 22301)». **Знати** стандарти організації процесів управління інцидентами кібербезпеки та забезпечення безперервності діяльності. **Вміти**: розробляти план реагування на інциденти, класифікувати їх та заповнювати відповідні звітні форми. **Формування компетентностей:** К31, КФ9. **Результати навчання:** РН2, РН14. **Рекомендовані джерела:** 1,4,8.			
Організація процесу управління інцидентами та забезпечення безперервності діяльності.	Лекція 11 2 год	-	Лекція-презентація, експрес-опитування здобувачів
Розробка плану реагування на інциденти кібербезпеки (Incident Response Plan).	Практичне заняття 8 2 год	2 бали	Отримання навичок розробки покрокового плану реагування на інциденти кібербезпеки (Incident Response Plan).
Моделювання класифікації інциденту та заповнення звітних форм за стандартом ISO 27035.	Лабораторне заняття 8 2 год	4 бали	Отримання навичок моделювання, класифікації кіберінциденту та заповнення звітних форм згідно зі стандартом ISO/IEC 27035.
Вивчення життєвого циклу управління інцидентами та роботи команд CERT/CSIRT.	Самостійна робота 8 3 год	-	Самостійна підготовка. Вивчення життєвого циклу управління інцидентами та регламентів роботи команд реагування (CERT/CSIRT).
Тема 9: «Стандарти захисту персональних даних та криптографії (GDPR, ISO/IEC 27701)». **Знати**: вимоги міжнародних стандартів та регламентів (зокрема GDPR) щодо захисту персональних даних та управління конфіденційністю. **Вміти**: проводити аудит процесів обробки даних та налаштовувати технічні засоби для забезпечення конфіденційності. **Формування компетентностей:** К39, КФ6. **Результати навчання:** РН1, РН7. **Рекомендовані джерела:** 1,13.			
Вимоги GDPR та стандартизація управління конфіденційністю (PIMS).	Лекція 12 2 год	-	Лекція-презентація, експрес-опитування здобувачів
Аудит процесів обробки даних на відповідність вимогам конфіденційності.	Практичне заняття 9 2 год	2 бали	Отримання навичок проведення аудиту процесів обробки персональних даних на відповідність вимогам конфіденційності (GDPR).

Налаштування технічних засобів забезпечення конфіденційності згідно зі стандартом.	Лабораторне заняття 9 2 год	4 бали	Отримання навичок налаштування технічних та організаційних засобів забезпечення конфіденційності згідно зі стандартом ISO/IEC 27701.
Підготовка до модульного контролю та підсумкового іспиту.	Самостійна робота 9 3 год	-	Самостійна підготовка. Узагальнення вивченого матеріалу. Підготовка до складання модульного контролю та підсумкового іспиту.
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Комп'ютерне обладнання, мультимедійний проектор, мережа Інтернет. Віртуальне навчальне середовище Google WorkSpace. Комп'ютерний клас з можливістю розгортання віртуальних машин для моделювання IT-інфраструктури (необхідно для практичної реалізації та тестування базових контролів безпеки CIS Controls). Спеціалізоване програмне забезпечення: інструменти для технічного аудиту інформаційної безпеки та перевірки налаштувань (наприклад, Nmap, OpenVAS, інструменти автоматизованого compliance-чекінгу). Навчальні зразки нормативно-технічної документації: шаблони Політик інформаційної безпеки, профілі захисту за НД ТЗІ, шаблони «Завдання з безпеки» (Security Target) за ISO 15408, матриці оцінки ризиків та «Положення про застосовність» (Statement of Applicability).			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			

1. Сучасні інформаційні технології в кібербезпеці [моногр.] / А.С. Довбиш, В.К. Ободяк, І.В. Шелехов. – Суми: СумДУ, 2021. – 348 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf
2. Технології захисту інформації в інформаційно-телекомунікаційних системах [навч. посіб.] / А.В. Жилін, О.М. Шаповал, О.А. Успенський. – К.: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
3. ДСТУ ISO/IEC 27000:2023 (ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник.
4. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. Режим доступу: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf
5. ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролю інформаційної безпеки.
6. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT). Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.
7. ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT). Інформаційні технології. Методи захисту. Критерії оцінювання безпеки IT (Common Criteria). Частина 1. Вступ і загальна модель.
8. Закон України «Про основні засади забезпечення кібербезпеки України». Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19
9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf
10. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf
11. NIST Cybersecurity Framework (CSF) Version 2.0. National Institute of Standards and Technology.
12. CIS Critical Security Controls (CIS Controls) Version 8. Center for Internet Security.
13. Загальний регламент про захист даних (GDPR) – Регламент (ЄС) 2016/679 Європейського Парламенту і Ради.

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

ПОТОЧНИЙ КОНТРОЛЬ			**Ви**
ПОТОЧНИЙ КОНТРОЛЬ	Виконання практичних робіт Виконання лабораторних робіт Модульна робота	18 балів 36 балів 6 балів	
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит*** **Додаткова оцінка**	• Метою *іспиту* є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків.	40 балів	
Види навчальної роботи			
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:			**Оц**
- 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		**100 БАЛІВ**	

БАЛИ

90-100			**Кр**
82-89	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)
75-81	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)
67-74	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)
60-66	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)
35-59	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє	**Середній**	Задовільно /

	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.	Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Зараховано (E)
0-34	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*
		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.