СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Корпоративна та професійна етика в кібербезпеці»

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, .		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** yushchavinsky@ukr.net; **сторінка курсу в Moodle –** Курс: Корпоративна та професійна етика в кібербезпеці (dut.edu.ua)	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	9	
Освітня програма			Інформаційна та кібернетична безпека		**Тип дисципліни**	основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	12	-	18	-	60

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у студентів базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою, умінь застосовувати знання для аналізу, супроводу і контролю ефективної роботи колективу, вирішення проблем та впровадження заходів протидії кіберінцидентам

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). КЗ6. Знання та розуміння предметної області і професійної 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, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ4**. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **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. **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)	
ПРН1. 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. **ПРН15**. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. **ПРН16.** Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. **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. **ПРН18.** Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
ЗМІСТОВИЙ МОДУЛЬ **1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»**			
Тема 1. Сучасна етика як практична філософія кібербезпеки ***Знати***: основні поняття предмету та завдань професійної та корпоративної етики; етичні засади науково-педагогічної діяльності; принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками. ***Вміти:*** володіти відповідним етичним інструментарієм для аналізу та прийняття рішень в конкретних ситуаціях професійної діяльності; застосовувати етичні норми при обґрунтовуванні використання, впровадженні та аналізі кращих світових стандартів, практик з метою розв'язання складних задач професійної діяльності в галузі управління інформаційною безпекою та кібербезпекою. ***Формування компетенцій:*** КЗ-1, КЗ-3, КЗ-5, КЗ-9, КФ1, КФ2, КФ10 ***Результати навчання:*** ПРН1, ПРН7, ПРН15 ***Рекомендовані джерела:*** 1-5, 19, 26, 28-31	Лекція 1 2 год	5*	Лекція-візуалізація
	Практичне заняття 1 2 год		Практична робота, Аналітичний метод Структура етичного знання: нормативна етика, професійна етика, корпоративна етика, етика наукової діяльності. Взаємозв'язок і взаємовплив моралі і права.
	Практичне заняття 2 2 год		Практична робота, проблемно-пошуковий метод Практичне використання етичних принципів у науково-педагогічній діяльності

Тема 2. Професійна та корпоративна етика в системі сучасного етичного знання. Професіоналізм як моральна цінність ***Знати***: принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками; актуальні механізми та інструменти морально-нормативної регуляції професійної діяльності та корпоративного управління. ***Вміти***: застосовувати етичні норми при обґрунтовуванні використання, впровадженні та аналізі кращих світових стандартів, практик з метою розв'язання складних задач професійної діяльності в галузі управління інформаційною безпекою та кібербезпекою. ***Формування компетенцій:*** КЗ-4, КЗ-5, КФ4, КФ7 ***Результати навчання:*** ПРН1, ПРН7 ***Рекомендовані джерела:*** 1-5, 19, 26, 28-31	Лекція 2 2 год	5*	Лекція-візуалізація
	Практичне заняття 3 2 год		Дедуктивний метод, Практична робота Професіоналізм як моральна риса особистості.
	Практичне заняття 4 2 год		Аналітичний метод, Практична робота Предмет та завдання корпоративної етики.
Тема 1. Сучасна етика як практична філософія кібербезпеки ***Тема 2. Професійна та корпоративна етика в системі сучасного етичного знання. Професіоналізм як моральна цінність***	Самостійна робота		Аналітичний метод, Практична робота 1. Структура етичного знання. 2. Нормативна етика, 3. Професійна етика, 4. Корпоративна етика, 5. Етика наукової діяльності 6. Поняття і принципи науково-педагогічної етики. 7. Етичний сенс глобальних проблем сучасної цивілізації. 8. Глобальні проблеми сучасного світу та перспективи їх розв'язання. 9. Професійна етика як спосіб регуляції поведінки в конкретних видах професійної діяльності. 10. Роль професійної та корпоративної етики в становленні професіоналізму Модульний контроль №1. 1. Виконання кваліфікаційних завдань. Тестування
ЗМІСТОВИЙ МОДУЛЬ **2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ»**			
Тема 3. ***Інформаційна етика*** ***Знати***: основи інформаційної етики, етичні норми концептуального підходу до побудови ефективної системи інформаційної безпеки.	Лекція 3 2 год	5*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5 2 год		Аналітичний метод, Практична робота Інформаційна етика в контексті змін у сучасному суспільстві.

Вміти: застосовувати знання етичних норм при створенні СУІБ і системи управління інцидентами інформаційної безпеки (СУІІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ. ***Формування компетенцій:*** КЗ-9, КФ1, КФ4 ***Результати навчання:*** ПРН7, ПРН15 ***Рекомендовані джерела:*** 1-5, 9, 10, 13, 23, 25, 28-31	Практичне заняття 6 2 год		Практична робота, проблемно-пошуковий метод Розвиток інформаційної етики як сучасного напряму етичної думки і типу моральної регуляції сучасного суспільства.
Тема 3. Інформаційна етика	Самостійна робота		Аналітичний метод, Практична робота 1. Інформаційна етика як моральна регуляція сучасного суспільства. 2. Інформаційне суспільство та інформаційна цивілізація. Інформаційна етика в просторі сучасних комунікативних процесів, в сучасній інформаційній та соціокультурній діяльності організацій. 3. Прикладна етика. 4. Аналіз інформаційної етики в контексті змін у сучасному суспільстві. 5. Розвиток інформаційної етики як сучасного напряму етичної думки і типу моральної регуляції сучасного суспільства
Тема 4. ***Професійна цифрова етика кібербезпеки*** ***Знати***: основи професійної комп'ютерної етики, етичні норми спілкування в соціальних мережах. ***Вміти***: застосовувати знання комп'ютерної етики в професійній діяльності при управлінні інформаційною безпекою організацій. ***Формування компетенцій:*** КФ1 ***Результати навчання:*** ПРН7, ПРН16 ***Рекомендовані джерела:*** 1-5, 8, 11,12, 23, 24, 25, 28-31	Лекція 4 2 год	5*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7 2 год		Практична робота, проблемно-пошуковий метод Хакерська етика. Переваги і недоліки. Обговорення результатів
	Практичне заняття 8 2 год		Практична робота, проблемно-пошуковий метод Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління інформаційною та кібербезпекою. Обговорення результатів
Тема 4. Професійна цифрова етика кібербезпеки	Самостійна робота		Практична робота 1. Поняття, принципи комп'ютерної етики. 2. Кодекс комп'ютерної етики. 3. Хакерська етика. 4. Філософія штучного інтелекту. 5. Етичні проблеми створення штучного розуму. 6. Комп'ютерна етика як професійна. 7. Етика інформаційної та кібербезпеки.

			8. Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління інформаційною та кібербезпекою
Тема 5. ***Корпоративні кодекси у сфері кібербезпеки*** ***Знати***: актуальні механізми та інструменти морально-нормативної регуляції професійної діяльності та корпоративного управління, принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками. ***Вміти***: розробляти корпоративну методику управління інформаційною безпекою на основі кращих світових практик впровадження систем управління в сфері безпеки, застосовувати знання етичних норм при розробленні корпоративних кодексів організацій і підприємств. ***Формування компетенцій:*** КЗ-7, КФ1, КФ2, КФ4 ***Результати навчання:*** ПРН16, ПРН18 ***Рекомендовані джерела:*** 6, 7, 18, 20, 21, 28-31	Лекція 5 2 год	5*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 9 2 год		Частково-пошуковий метод Практична робота Функції, які виконують корпоративні кодекси в організаціях. Обговорення результатів
	Практичне заняття 10 2 год		Практична робота, Частково-пошуковий метод Професійні кодекси в сфері ІТ, інформаційній та кібернетичній безпеці. Обговорення результатів
Тема 5. Корпоративні кодекси у сфері кібербезпеки	Самостійна робота		Практична робота 1. Поняття «кодексу корпоративної етики». 2. Типи корпоративних кодексів. 3. Основні функції, які виконують корпоративні кодекси в організаціях. 4. Характеристики відмінного кодексу. 5. Професійні кодекси в сфері ІТ, інформаційній та кібернетичній безпеці. 6. Особливості впровадження кодексів корпоративної етики у провідних компаніях світу та в Україні.
Тема 6. ***Етика конфлікту та методології прийняття етичних рішень в професійних ситуаціях управління кібербезпекою*** ***Знати***: види, причини конфліктів в управлінні кібербезпекою, методи їх вирішення. ***Вміти***: вирішувати конфлікти із застосуванням етичних норм, застосовувати знання етичних норм при створенні СУІБ і системи управління інцидентами інформаційної безпеки (СУІІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ,	Лекція 3 2 год	5*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5 2 год		Частково-пошуковий метод Метод "мозкового штурму" Конфлікти в управлінні кібербезпекою та методи їх визначення. Обговорення результатів
	Практичне заняття 6 2 год		Метод сценаріїв, Метод "теорії ігор" Застосування етичних методів і засобів при управлінні інформаційними інцидентами і ризиками. Обговорення результатів

володіти відповідним етичним інструментарієм для аналізу та прийняття рішень в конкретних ситуаціях професійної діяльності. ***Формування компетенцій:*** КЗ-8, КЗ-9, КФ7, КФ10 ***Результати навчання:*** ПРН15,ПРН16,ПРН18 ***Рекомендовані джерела:*** 22, 14-17, 26-31			
Тема 6. Етика конфлікту та методології прийняття етичних рішень в професійних ситуаціях управління кібербезпекою	Самостійна робота		Частково-пошуковий метод Практична робота 1. Методи вивчення конфлікту. 2. Види та сутність конфліктів. 3. Методологічні засади конфліктології. 4. Методи подолання конфліктів. 5. Виокремлення наявних та потенційних моральних проблем в організації інформаційної безпеки корпорацій. 6. Етичні методи і засоби управління інформаційними інцидентами і ризиками, способи вирішення складних етичних ситуацій в управлінні інформаційною та кібербезпекою. 7. Використання відповідного етичного інструментарію для аналізу та прийняття рішень в конкретних ситуаціях професійної та ділової діяльності. 8. Етика конфлікту та методології прийняття етичних рішень в професійних ситуаціях. Модульний контроль №2. 1. Виконання кваліфікаційних завдань. Тестування

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
- програмне забезпечення перевірки СУІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Бралатан В. П., Гуцаленко Л. В., Здирко Н. Г. Професійна етика: Навч. посібник.- К.:Центр учбової літератури, 2011. – 252 с.
2. О. Левицька. Професійна етика // Філософський енциклопедичний словник / В. І. Шинкарук (гол. редкол.) та ін. — Київ : Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. — С. 531. — 742 с. — 1000 екз. — ББК 87я2. — ISBN 966-531-128-X.
3. Davis, Michael (2003 р.). Language of professional ethics (Мова професійної етики). Доступно за посиланням: http://ethics.iit.edu/teaching/language-professionalethics.
4. Weil, Vivian (2008 р.). Professional ethics (Професійна етика). Доступно за посиланням: http://ethics.iit.edu/teaching/professional-ethics.
5. Етика. Естетика.: навч.посібник. / за наук. ред.Панченко В. І. – К.: «Центр учбової літератури», 2014 – 432 с.
6. Професійна та корпоративна етика: навч. посіб. / за ред., В.І. Панченко. – К: 2019 ВПЦ «Київський університет», 2019 – 392 с..

7. Ломачинська І.М., Рихліцька О.Д., Барна Н.В. Основи корпоративної культури.// Навч. посібник. – К.: 2011., – 480 с.
8. Уэбстер Ф. Теорії інформаційного суспільства. – К., 2004. (переклад з англ.)
9. Савченко В. А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Савченко В. А., Савченко В. В., Довбешко С. В., Мацько О. Й., Зідан А. М. // Сучасний захист інформації №4(36), 2018, – С. 40-49.
10. Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу / Савченко В. А., Мацько О. Й. // Сучасний захист інформації №2(38), 2019 – С. 6-16.
11. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.
12. Савченко В. А.Модель інформаційного стримування між державами на основі теорії рефлексивних ігор / Савченко В. А., Дзюба Т. М. //Сучасний захист інформації №2(42), 2020. С. 6-18.
13. ДСТУ ISO/IEC 27035-1:2018.Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами(ISO/IEC 27035-1:2016, IDT).
14. ДСТУ ISO/IEC 27035-1:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. (ISO/IEC 27035-1:2016, IDT).
15. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).
16. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).
17. Герчанівська П. Е. Культура управління : навч. посібник / Герчанівська П. Е. – К. : ІВЦ Видавництво "Політехніка", 2005. – 152 с.
18. Гах Й. М. Етика ділового спілкування : навч. посібник / Гах Й. М. – К. : Центр навч. літератури, 2005. – 160 с.
19. Ложкін Т. В. Психологія конфлікту: теорія і сучасна практика : навч. посібник / Т. В. Ложкін, Н.І. Пов'якель. – К. : ВД «Професіонал», 2006. – 416 с.
20. Морозова Т. Ю. Про необхідність вивчення комп'ютерної етики майбутніми ІТ-фахівцями / Т. Ю. Морозова // [Електрон.ресурс].-Спосіб доступу: http://www.nbuv.gov.ua/portal/natural/vkpi/FPP/2006- 2/05Morozova.pdf.
21. Філіпова Л. Я. Комп'ютерна етика, інформаційна етика та кіберетика: сутність та співвідношення понять. Інформаційна діяльність: Проблеми науки, освіти та практики: матеріали міжнар. наук.-практ. конф.— К, ДАКККМ, 2009. — С.137-140.
22. Филиппова Л. Я., Зеленецкий В. С. Ккомп'ютерна етика. Морально-етичні і правові норми для користувачів комп'ютерних мереж: Навч. посібник. — Харків: Вид-во «Кроссроуд», 2006. — 209 с.
23. Якименко Ю. М. Про підхід до створення системи інформаційної безпеки в організації. Інформаційна безпека України: Зб. наук. доп. та тез НТК. Київ: Київський національний університет імені Тараса Шевченка(23-24 березня 2017року). С. 372-376.
24. Якименко Ю. М. Використання метрик для оцінки ефективності управління інцидентами інформаційної безпеки. Матеріали: інтернет-конференція «Актуальні проблеми інформаційної та кібернетичної безпеки»(26 жовтня 2018 року). Тези доповідей. Київ: ДУТ(ННІЗІ), 2018. С.69-71.
25. Інформаційні ресурси
26. Тексти лекцій та практичних занять (електронний варіант).
27. Електронна бібліотека ДУТ.
28. Електронні матеріали в MOODLE : Курс: Корпоративна та професійна етика в кібербезпеці (dut.edu.ua)
29. Інтернет-ресурси:

http://www.nbuv.gov.ua/ - сайт Національної бібліотеки України
http://www.scientific-library.net –Электронна бібліотека науково-технічної літератури
https://www.unodc.org/documents/e4j/IntegrityEthics/E4J_Integrity_and_Ethics_Module_14_final_UKR.pdf – професійна етика
https://kneu.edu.ua/ua/science_kneu/ndi/prikl_etiki/ - сайт інституту прикладної та професійної етики

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.

- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»»	максимальна оцінка – 15балів
	Модульний контроль № 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ»	максимальна оцінка –15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
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

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об 'єктів діяльності фахівця на основі набутих з даної та	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка	Відмінно / Зараховано (А)

	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.	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)

64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі іспиту.	**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*