Затверджено
Завідувач кафедри УКБЗІ_____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

”КОРПОРАТИВНА ТА ПРОФЕСІЙНА ЕТИКА В КІБЕРБЕЗПЕЦІ”

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, доцент		**Контактна інформація лектора (e-mail), сторінка курсу на платформі GWE**	**e-mail:** y.shchavinskyi@duikt.edu.ua **сторінка курсу в GWE –** https://classroom.google.com/c/NzA3Mjc3OTY5MDYx?cjc=phss4af	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1	
Освітньо-професійна програма			Управління інформаційною та кібернетичною безпекою Інформаційна та кібернетична безпека		**Тип дисципліни**	Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	12	-	18	-	60

АНОТАЦІЯ КУРСУ

Освітні компоненти для яких є базовою	1. Педагогіка та психологія у вищій школі. 2. Управління проєктами інформаційної безпеки. 3. Науково-педагогічна практика, 4. Науково-дослідна практика
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 етичних проблем та впровадження заходів протидії кіберінцидентам

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. **КЗ 3.** Здатність до абстрактного мислення, аналізу та синтезу. **КЗ 4.** Здатність оцінювати та забезпечувати якість виконуваних робіт. **КЗ 5.** Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	**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. **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 (РН)	
РН 1. 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. **РН 7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **РН 15.**. 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. **РН 16.** 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. **РН 18.** 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
Розділ **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	Лекція 1 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 1 2 год		Усне опитування, розв'язання практичних завдань. Практичне використання етичних принципів у науково-педагогічній діяльності
	Самостійна робота 8 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки

професійної діяльності в галузі управління інформаційною безпекою та кібербезпекою. ***Формування компетенцій:*** К31, К33, К35, КФ2, КФ10 ***Результати навчання:*** РН1, РН7, РН15 ***Рекомендовані джерела:*** 1-5, 19, 25-26, 31-32			сучасного підприємства з врахуванням впливу факторів зовнішнього середовища.
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:*** К31, К35, КФ4 ***Результати навчання:*** РН1, РН7, РН15, РН16 ***Рекомендовані джерела:*** 1-5, 19, 25-26, 29-32	Лекція 2 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 2 2 год		Усне опитування, тематична навчальна дискусія, розв'язання практичних завдань з обгрунтування кращих світових стандартів та практик управління кібербезпекою
	Самостійна робота 8 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки сучасного підприємства з врахуванням впливу факторів зовнішнього середовища. Виконання кваліфікаційних завдань. Тестування
Розділ **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. ***Вміти***: застосовувати знання етичних норм при створенні системи управління інцидентами інформаційної безпеки (СУІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ. ***Формування компетенцій:*** К31, К35, КФ4 ***Результати навчання:*** РН7, РН16 ***Рекомендовані джерела:*** 1-5, 9, 10, 13, 23, 25-26, 31	Лекція 3 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 3 2 год		Усне опитування, тематична навчальна дискусія, розв'язання практичних завдань застосування етичних норм при створенні СУІБ і системи управління інцидентами інформаційної безпеки.
	Самостійна робота 8 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки сучасного підприємства з врахуванням впливу факторів зовнішнього середовища.

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:*** К31, КФ2 ***Результати навчання:*** РН7, РН16 ***Рекомендовані джерела:*** 1-5, 8, 11,12, 23, 24, 25-26	Лекція 4 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 4 2 год		Усне опитування, тематична навчальна дискусія, розв'язання практичних завдань в застосуванні методів та механізмів розв'язання основних моральних дилем цифрової етики
	Практичне заняття 5 2 год		Усне опитування, тематична навчальна дискусія, розв'язання ситуативних практичних завдань моніторингу соціальних мереж
	Самостійна робота 12 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки сучасного підприємства з врахуванням впливу факторів зовнішнього середовища.
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:*** К31, КФ2, КФ4 ***Результати навчання:*** РН7, РН16, РН18 ***Рекомендовані джерела:*** 6, 7, 18, 20, 21, 25-26	Лекція 5 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 6 2 год		Усне опитування, тематична навчальна дискусія, розв'язання практичних завдань застосування механізмів та інструментів морально-нормативної регуляції в корпоративному управлінні кібербезпекою.
	Практичне заняття 7 2 год		Усне опитування, тематична навчальна дискусія, розв'язання практичних завдань застосування етичних норм при створенні професійних та корпоративних кодексів в сфері ІТ, інформаційній та кібернетичній безпеці. Обговорення результатів.
	Самостійна робота 12 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки сучасного підприємства з врахуванням впливу факторів зовнішнього середовища.
Тема 6. ***Етика конфлікту та методи прийняття етичних рішень в професійних ситуаціях управління кібербезпекою***	Лекція 6 2 год	10 балів	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів

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, володіти відповідним етичним інструментарієм для аналізу та прийняття рішень в конкретних ситуаціях професійної діяльності. ***Формування компетенцій:*** К31, К33, К35, КФ2, КФ4, КФ10 ***Результати навчання:*** РН1, РН7, РН15, РН16, РН18 ***Рекомендовані джерела:*** 22, 14-17, 25-26	Практичне заняття 8 2 год		Усне опитування, тематична навчальна дискусія, розв'язання ситуативних завдань вирішення конфліктних ситуацій в управлінні кібербезпекою. Обговорення результатів
	Практичне заняття 9 2 год		Метод сценаріїв, Метод "теорії ігор". Усне опитування, тематична навчальна дискусія, розв'язання конфліктів при управлінні інформаційними інцидентами і ризиками у відповідності з етичними нормами міжнародних стандартів. Обговорення результатів
	Самостійна робота 12 год		Робота з конспектами лекцій. Аналітична обробка додаткового матеріалу. Удосконалення отриманих знань та умінь, отриманих за попередніми лекцією та практичним заняттям щодо формування життєвого циклу проєкту кібербезпеки сучасного підприємства з врахуванням впливу факторів зовнішнього середовища. 1. Виконання кваліфікаційних завдань. Тестування

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки
- навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center)
- академічний центр компетенцій IBM «Кіберполігон»
- програмно-апаратні комплекси: IBM QRadar SIEM; IBM i2 Analyze Notebook Premium; Tenable Nessus Professional; ESET Protection.
- програмний комплекс для організації дистанційного навчання в мережі Internet GWE.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Легомінова С.В., Щавінський Ю.В., Мужанова Т.М., Якименко Ю.М., Капелюшна Т.В., Рабчун Д.І. Професійна етика управлінської діяльності в кібербезпеці. навч. посіб. Київ : ДУТ, 2023, 198 с.
2. Бралатан В. П., Гуцаленко Л. В., Здирко Н. Г. Професійна етика: Навч. посібник.- К.:Центр учбової літератури, 2011. – 252 с.
3. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навч. посіб. Київ : ДУТ, 2023. 125 с.
4. Якименко Ю. М., Легомінова С. В., Щавінський Ю. В., Рабчун Д. І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби : навч. посіб. Київ : ДУТ, 2023. 243 с.
5. Мужанова Т.М., Щавінський Ю.В., Рабчун Д.І. Управління безпекою інформаційних мереж: навч. посіб. Київ : ДУТ, 2023. 167 с.
6. 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.
7. Davis, Michael (2003 p.). Language of professional ethics (Мова професійної етики). URL: http://ethics.iit.edu/teaching/language-professionalethics.

8. Weil, Vivian (2008 р.). Professional ethics (Професійна етика). URL:: http://ethics.iit.edu/teaching/professional-ethics.
9. Етика. Естетика.: навч.посібник. / за наук. ред.Панченко В. І. – К.: «Центр учбової літератури», 2014 – 432 с.
10. Професійна та корпоративна етика: навч. посіб. / за ред., В.І. Панченко. – К: 2019 ВПЦ «Київський університет», 2019 . 392 с..
11. Ломачинська І.М., Рихліцька О.Д., Барна Н.В. Основи корпоративної культури. Навч. посібник. К.: 2011., 480 с.
12. Уэбстер Ф. Теорії інформаційного суспільства. К., 2004. (перегkfl з англ)
13. 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.
14. 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.
15. 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 .
16. 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.
17. 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).
18. 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).
19. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).
20. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).
21. Герчанівська П. Е. Культура управління : навч. посібник / Герчанівська П. Е. – К. : ІВЦ Видавництво “Політехніка”, 2005. 152 с.
22. Гах Й. М. Етика ділового спілкування : навч. посібник / Гах Й. М. – К. : Центр навч. літератури, 2005. – 160 с.
23. Ложкін Т. В. Психологія конфлікту: теорія і сучасна практика : навч. посібник / Т. В. Ложкін, Н.І. Пов’якель. К. : ВД «Професіонал», 2006. 416 с.
24. Морозова Т. Ю. Про необхідність вивчення комп’ютерної етики майбутніми ІТ-фахівцями / Т. Ю. Морозова URL: http://www.nbuv.gov.ua/portal/natural/vkpi/FPP/2006- 2/05Morozova.pdf .
25. 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.
26. Филиппова Л. Я., Зеленецкий В. С. Комп’ютерна етика. Морально-етичні і правові норми для користувачів комп’ютерних мереж: Навч. посібник. Харків: Вид-во «Кроссроуд», 2006. 209 с.
27. 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.
28. 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.
29. Shchavinsky Yu. Application of ethical principles in cybersecurity. Modern vision of implementing innovations in scientific studies: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, July 25, 2025. Marseille, French Republic: International Center of Scientific Research. pp. 83-87. URL: https://doi.org/10.36074/scientia-25.07.2025
30. Lehominova S.V., Shchavinsky Y.V., Budaretsky Y.I., Budzynsky O.V. Application of artificial intelligence for automated assessment of situational tasks in cybersecurity training. Наукові записки ДУІКТ . 2025. No 1 (7). P. 57-67. URL: https://doi.org/10.31673/2786-8362.2025.012293

31. Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. Модель оцінювання етичної зрілості системи інформаційної безпеки організації. Телекомунікаційні та інформаційні технології. 2025. № 3. С. 194-203. URL: https://doi.org/10.31673/2412-4338.2025.038722
32. Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації. 2025. № 3(63). С. 90–98. URL: https://doi.org/10.31673/2409-7292.2025.031152

Інформаційні ресурси

Інформаційні технології у психології ч. 2. Електронний навчально-методичний комплекс /Щавінський Ю.В., Баранюк Н.І.// Львів : Національний університет «Львівська політехніка», 2018. № Е41-139-326/2020 від 12.10.2020 Тексти лекцій та практичних занять (електронний варіант).

Електронна бібліотека ДУІКТ.

Електронні матеріали в GWE : https://classroom.google.com/c/NzA3Mjc3OTY5MDYx?cjc=phss4af

Інтернет-ресурси:

http://www.nbuv.gov.ua/ - сайт Національної бібліотеки України

http://www.scientific-library.net – Електронна бібліотека науково-технічної літератури

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 за темами:***	
	Тема 1. Сучасна етика як практична філософія кібербезпеки	10 балів
	Тема 2. Професійна та корпоративна етика в системі сучасного етичного знання. Професіоналізм як моральна цінність	10 балів
	Тема 3. Інформаційна етика	10 балів
	Тема 4. Професійна цифрова етика кібербезпеки	10 балів
	Тема 5. Корпоративні кодекси у сфері кібербезпеки	10 балів
	Тема 6. Етика конфлікту та методи прийняття етичних рішень в професійних ситуаціях управління кібербезпекою	10 балів

	порядок оцінювання на заняттях : • 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 ДОДАТКОВО за участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо. 5-10 балів	
	ВСЬОГО ЗА ПОТОЧНИЙ КОНТРОЛЬ	60 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій або у тестовій формі	40 балів
ВСЬОГО		100 балів

ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Виконання навчальних завдань на практичних заняттях та під час самостійної підготовки, проведення поточного контролю результатів навчання, з використанням самостійних (індивідуальних) форм роботи, зокрема за допомогою системи **GWE** перевіряється **на плагіат у відповідності з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій https://duikt.edu.ua/uploads/p_447_96297052.pdf?2**

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 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	**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 вивчається.	Відмінно / Зараховано (А)

	чи складних практичних завдань.		
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	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

	формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.		
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*
ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ			
Виконання навчальних завдань на практичних заняттях та під час самостійної підготовки, проведення поточного контролю результатів навчання, з використанням самостійних (індивідуальних) форм роботи, зокрема за допомогою системи **GWE** перевіряється **на плагіат у відповідності з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій** https://duikt.edu.ua/uploads/p_447_96297052.pdf?2		