Затверджено
Завідувач кафедри УКБЗІ _____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, доцент .		**Контактна інформація лектора (e-mail), сторінка курсу GWE**	**e-mail:** y.shchavinskyi@duikt.edu.ua **сторінка курсу в GWE – https://classroom.google.com/c/NzA3MzAyODc2OTc1**	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1	
Освітня програма			Інформаційна та кібернетична безпека; Управління кібербезпекою та захистом інформації; Управління інформаційною та кібернетичною безпекою Технічні системи інформаційного та кібернетичного захисту Системи кіберзахисту та реагування на інциденти		**Тип дисципліни**	Обов’язкова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Базова
Освітні компоненти, для яких є базовою	1. Стандарти кібербезпеки та захисту інформації. 2. Інформаційна безпека держави. 3. Організація конфіденційного діловодства

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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, доцент .		**Контактна інформація лектора (e-mail), сторінка курсу GWE**	**e-mail:** y.shchavinskyi@duikt.edu.ua **сторінка курсу в GWE – https://classroom.google.com/c/NzA3MzAyODc2OTc1**	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1	
Освітня програма			Інформаційна та кібернетична безпека; Управління кібербезпекою та захистом інформації; Управління інформаційною та кібернетичною безпекою Технічні системи інформаційного та кібернетичного захисту Системи кіберзахисту та реагування на інциденти		**Тип дисципліни**	Обов’язкова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Базова
Освітні компоненти, для яких є базовою	1. Стандарти кібербезпеки та захисту інформації. 2. Інформаційна безпека держави. 3. Організація конфіденційного діловодства

Мета курсу:	формування у студентів необхідної системи знань з основ національного та міжнародного законодавства, яке регулює правові відносини в інформаційній сфері, визначає сутність та зміст механізмів забезпечення інформаційної безпеки, світогляду щодо сфери забезпечення інформаційної безпеки, різновидів завдань інформаційної безпеки та способів їх вирішення; здобуття теоретичних знань, умінь, навичок та інших компетентностей щодо використання правових механізмів захисту інформації та вирішення інших завдань інформаційної безпеки

Компетентності відповідно до освітньої програми	
Інтегральна компетентність	
ІК. Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	
Soft- skills /Загальні компетентності (ЗК)	**Hard-skills / Спеціальні (фахові, предметні) компетентності (СК)**
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	**СК1.** Здатність застосовувати законодавчу нормативно-правову базу, а також державні міжнародні вимоги
Програмні результати навчання (РН)	
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ **1. Теоретичні основи правового забезпечення інформаційної безпеки**			
Тема №1. Сутність та основні поняття нормативно-правового забезпечення інформаційної безпеки ***Знати***: сутність та основні поняття нормативно-правового забезпечення інформаційної безпеки, характеристику діяльності міжнародних організацій щодо правого забезпечення міжнародної інформаційної безпеки ***Вміти:*** характеризувати діяльність організацій щодо правого забезпечення інформаційної безпеки з урахуванням міжнародного досвіду . ***Формування компетенцій:*** ІК, ЗК6 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 15, 26, 28-31	Лекція 1 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 1 2 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод 1. Характеристика діяльності міжнародних організацій щодо правого забезпечення міжнародної інформаційної безпеки.
	Самостійна робота 6 год		Аналітичний метод, самостійне виконання завдання 1. Принципи та джерела правового забезпечення інформаційної безпеки в Україні
Тема №2. Інформаційна безпека в системі складових національної безпеки України ***Знати***: роль та місце інформаційної безпеки в системі складових Національної безпеки України, зміст основних	Лекція 2 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 2 2 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод

документів щодо інформаційної безпеки, як складової Національної безпеки України.			1. Інформаційне суспільство: сутність та основні напрями розвитку
Вміти: аналізувати основні загрози національній безпеці України в інформаційній сфері ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 15, 26, 28-31, 44-46	Самостійна робота 6 год		Аналітичний метод, самостійне виконання завдання 1. Аналіз основних загроз інформаційній безпеці України та відповідних пріоритетів державної політики
Тема №3. Інформація та інформаційні ресурси як об'єкт правових відносин. ***Знати***: визначення та характерні риси інформаційного суспільства, характеристику основних напрямів розвитку інформаційного суспільства, нормативно-правове забезпечення розвитку інформаційного суспільства в Україні, значення інформаційної безпеки для розвитку інформаційного суспільства в Україні. ***Вміти:*** характеризувати діяльність організацій щодо правого забезпечення інформаційної безпеки з урахуванням міжнародного досвіду . ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 15, 26, 28-31	Лекція 3 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 3 2 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод 1 Діджиталізація України та інформаційна безпека.
	Самостійна робота 6 год		Аналітичний метод, самостійне виконання завдання 1. Інформація та інформаційні ресурси як об'єкт правових відносин.
Розділ **2. Нормативно-правове забезпечення безпеки людини, суспільства та держави**			
Тема №4. Інформаційна війна та інформаційний тероризм, як основні загрози безпеці людини, суспільства та держави. ***Знати***: види інформаційної війни, суть інформаційного тероризму, основні загрози безпеці людини, суспільства та держави, правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни, способи боротьби з пропагандою та неправдивою (фейковою) інформацією, ***Вміти***: застосовувати способи боротьби з пропагандою та неправдивою (фейковою) інформацією при виконанні функціональних обов'язків, ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 13-14, 16-38	Лекція 4 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 4 2 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод 1.Правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни.
	Самостійна робота 6 год		1. Аналітичний метод, самостійне виконання завдання Механізми боротьби з інформаційним тероризмом

Тема №5. Правове регулювання захисту персональних даних в Україні ***Знати***: сутність та основні поняття нормативно-правового забезпечення захисту персональних даних, характеристику діяльності міжнародних організацій щодо правого забезпечення міжнародної інформаційної безпеки ***Вміти:*** організовувати і контролювати заходи захисту персональних даних в організаціях . ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 15, 26, 28-31, 42	Лекція 5 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 5 2 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод 1.Медіаграмотність громадян як основний спосіб захисту від маніпулювання суспільною свідомістю.
	Самостійна робота 6 год		Аналітичний метод, самостійне виконання завдання 1. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.
Тема №6. Регулювання використання та розвитку мережі Інтернет ***Знати***: механізми правового регулювання прав дотримання прав людини в Інтернет, способи боротьби з пропагандою та неправдивою (фейковою) інформацією, ***Вміти***: застосовувати способи боротьби з пропагандою та неправдивою (фейковою) інформацією при виконанні функціональних обов'язків ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-12, 13-14, 16-38, 41-43	Лекція 6 2 год	5 балів	Лекція-візуалізація
	Практичне заняття 6 2 год		Дедуктивний метод, Практична робота 1.Способи боротьби з пропагандою та неправдивою (фейковою) інформацією.
	Самостійна робота 6 год		Аналітичний метод, самостійне виконання завдання 1. Права людини в Інтернет
Розділ **3. Нормативно-правове забезпечення кібербезпеки**			
Тема №7. Національна система кібербезпеки України ***Знати***: склад і структуру національної системи кібербезпеки України, форми і способи боротьби у кіберпросторі, сутність і зміст викликів та загроз кібербезпеці України, напрями державної політики України щодо кіберзахисту об'єктів критичної інфраструктури ***Вміти***: визначати пріоритети забезпечення кібербезпеки об'єктів критичної інфраструктури, застосовувати знання при створенні СУІБ і системи управління інцидентами інформаційної безпеки (СУІІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою. ***Формування компетенцій:*** ІК, ЗК6, СК1	Лекція 7 2 год	5 балів	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7 2 год		Аналітичний метод, Практична робота 1.Сутність і зміст викликів та загроз кібербезпеці України.
	Самостійна робота 6 год		Практична робота, аналітичний, частково-пошуковий метод 1. Захист інтелектуальної власності в Україні.

Результати навчання: РН9 ***Рекомендовані джерела:*** 1-15, 17-38, 39-43, 45, 46			
Тема №8. Правове забезпечення захисту інформації в Україні. ***Знати***: види кіберзлочинів, основи правового регулювання боротьби з кіберзлочинністю, напрями державної політики України щодо кіберзахисту об'єктів критичної інфраструктури, напрями застосування штучного інтелекту в боротьбі з кіберзлочинами ***Вміти***: класифікувати та розслідувати кіберзлочини, організовувати державно-приватне партнерство у сфері кібербезпеки в нормативно-правовому полі, визначати вразливості критичної інфраструктури, ідентифікувати загрози критичної інфраструктури ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-15, 17-38, 44-46	Лекція 8 2 год Практичне заняття 8 2 год Самостійна робота 6 год	5 балів	Лекція-візуалізація, експрес-опитування Аналітичний метод, самостійне виконання завдання 1. Нормативно-правове забезпечення захисту, безпеки та стійкості критичної інфраструктури. Практична робота, аналітичний, частково-пошуковий метод 1. Правове регулювання захисту інформаційного простору України від негативного інформаційно-психологічного впливу
Тема №9. Стандарти інформаційної безпеки ***Знати***: сутність та зміст стандартів забезпечення кібербезпеки, міжнародні та національні стандарти забезпечення кібербезпеки, сутність та зміст ліцензування та сертифікації діяльності у сфері кібербезпеки, види сертифікатів та ліцензій на діяльність у сфері кібербезпеки ***Вміти***: організовувати правове забезпечення технічного захисту інформації, правове забезпечення криптографічного захисту інформації в інформаційно-телекомунікаційних системах. ***Формування компетенцій:*** ІК, ЗК6, СК1 ***Результати навчання:*** РН9 ***Рекомендовані джерела:*** 1-15, 17-38, 40-43	Лекція 9 2 год Практичне заняття 9 2 год Самостійна робота 6 год	5 балів	Лекція-візуалізація, експрес-опитування Аналітичний метод, Практична робота 1.Пріоритети забезпечення кібербезпеки України Практична робота, аналітичний, частково-пошуковий метод 1. Стандарти інформаційної безпеки
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

Базова

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки». URL: https://zakon.rada.gov.ua/laws/show/537-16#Text
4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
7. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
10. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037
11. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
12. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069
13. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ:КВІЦ, 2019. 344 с..URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf
14. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: монографія/О.Д. Довгань, І.М.Доронін; НАРН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107с. URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf
15. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315;

Допоміжна

16. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;
17. Закон України «Про боротьбу з тероризмом»;
18. Закон України «Про авторське право та суміжні права»;
19. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних»;
20. Указ Президента України від 23 листопада 2011 року 1067/2011 «Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації»
21. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року N 1229/99;
22. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року N 505/98;
23. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518;
24. Міжнародні стандарти серії ISO/IEC 2700x:2018 «Information technology. Security techniques»;

25. Стандарт безпеки даних індустрії платіжних карток Payment Card Industry Data Security Standard (PCI DSS);
26. Стандарти інформаційної безпеки США NIST Special Publications 800 Series;
27. Відкритий IT-стандарт Асоціації з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI) CoBiT (Control Objectives for Information and Related Technology – «Контрольні цілі для інформаційних та суміжних технологій»);
28. Загальний регламент про захист даних ЄС GDPR (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679
29. Указ Президента України від 15 травня 2017 року № 133/2017 «Про введення в дію Рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»;
30. Наказ Служби безпеки України від 12.08.2005 № 440 «Про затвердження Зводу відомостей, що становлять державну таємницю»;
31. Указ Президента України від 29.10.2014 № 828/2014 «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації»;
32. Постанова Кабінету Міністрів України від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
33. Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»
34. Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»
35. Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»
36. Постанова Кабінету Міністрів України від 04.04.2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»
37. Наказ Адміністрації ДССЗЗІ України від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
38. Наказ Адміністрації ДССЗЗІ України від 06.10.2021 № 601 «Про затвердження методичних рекомендацій щодо підвищення рівня кібербезпеки»
39. Наказ Адміністрації ДССЗЗІ України від 03.07.2023 № 570 «Про затвердження методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»
40. Наказ Адміністрації Держспецзв'язку від 11.07.2025 № 424 «Про затвердження Порядку ведення переліку авторизованих систем з безпеки»
41. Наказ Адміністрації Держспецзв'язку від 14.01.2025 № 17 «Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів ...
42. Наказ Адміністрації Держспецзв'язку від 05.08.2025 № 482 «Про затвердження Методичних рекомендацій щодо збору та обробки статистичних даних стосовно кібератак, кіберінцидентів і заходів протидії у Державній службі спеціального зв'язку та захисту інформації України»
43. Окінавська хартія глобального інформаційного суспільства.
44. Мужанова, Т., Легомінова, С., Капелюшна, Т., Щавінський, Ю., & Запорожченко, М. (2026). Особливості сучасних кібероперацій за підтримки держав як новітньої форми міждержавного протиборства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(32), 71–89. https://doi.org/10.28925/2663-4023.2026.32.1116
45. Мужанова, Т., Легомінова, С., Щавінський, Ю., Якименко, Ю., & Нестеренко, Г. (2024). Основні підходи й напрями розвитку політики кібербезпеки європейського союзу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 133–149. https://doi.org/10.28925/2663-4023.2024.24.133149
46. Lehominova S.V., Shchainskyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in Ukraine in the conditions of hybrid war. Телекомунікаційні та інформаційні технології, №1(2023). С. 101-110 https://doi.org/10.31673/2412-4338.2023.0101111

Інформаційні ресурси

1. Презентації лекцій та практичних занять (електронний варіант).

2. Електронна бібліотека ДУІКТ.
3. Інтернет-ресурси:
   - Міжнародні договори, що набули чинності для України та включені до Єдиного державного реєстру нормативно-правових актів (по роках: 1991 – 2022). Сайт Міністерства юстиції України: https://minjust.gov.ua/;
   - Зібрання чинних міжнародних договорів України. Сайт Верховної Ради України, URL: https://zakon.rada.gov.ua/laws/main/b94 ;
   - Зібрання навчальних матеріалів державної освітньої програми «Дія. Цифрова освіта» URL: https://osvita.diia.gov.ua/;
   - Онлайн-бібліотека з питань медіаграмотності та інформаційної безпеки Міністерства культури та інформаційної політики України. URL: https://mip.gov.ua/news/10/;

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
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій у фахових виданнях, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за тематикою дисципліни, створення кейсів	Звільняється від іспиту

Поточна оцінка	Сума оцінок за кожну тему 45 балів Індивідуальне завдання (реферат) 15 балів	60 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Екзамен***	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Екзамен проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			**100 балів**
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 чи складних практичних завдань.	**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)
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 (В)
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/	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають	Добре / Зараховано (С)

	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.	утруднення.	
67-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. 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