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

СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ
«Методи та засоби протидії кібезлочинності»

Лектор курсу			Капелюшна Тетяна Вікторівна, доктор економічних наук, доцент, професор кафедри управління кібербезпекою та захистом інформації		Контактна інформація лектора (e-mail), сторінка курсу в GWE	e-mail: t.kapeliushna@duikt.edu.ua сторінка курсу в GWE - https://classroom.google.com/c/ODA1NTM1MzAxMzMz	
Галузь знань			12 Інформаційні технології		**Освітній рівень**	бакалавр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**		
Освітньо-професійна програма			Управління кібербезпекою та захистом інформації Управління інформаційною та кібернетичною безпекою Інші ОП		**Тип дисципліни**	вибіркова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	18	18	-	96

АНОТАЦІЯ КУРСУ

Мета курсу:	надати студентам системні знання щодо організаційних і технічних аспектів протидії кіберзлочинності та сформувати практичні навички роботи з інструментами аналізу кіберінцидентів, цифрових доказів і засобів кіберзахисту..

Компетенції відповідно до освітньо-професійної програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні (фахові) компетенції**
ІК Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	
ЗК1. Здатність застосовувати знання у практичних ситуаціях **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності	**СК2.** Здатність до використання інформаційних технологій, сучасних методів і моделей кібербезпеки та систем захисту інформації. **СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою

Результати навчання відповідно до освітньо-професійної (програмні результати навчання – ПРН)

РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Політика оцінювання за темою	Форми і методи навчання/питання до самостійної роботи
Розділ 1. Теоретичні засади протидії кібезлочинності			
Тема 1. **Вступ до кіберзлочинності: класифікація, тенденції, правові засади** ***Знати***: класифікацію кіберзлочинів та їх хаактеристики; основні міжнародні акти у сфері протидії кіберзлочинності (Будапештська конвенція); суб'єктів протидії кіберзлочинності: державні та приватні структури; тенденції розвитку кіберзлочинності ***Вміти:*** застосовувати правові норми до класифікації кіберінцидентів; розрізняти види кіберзлочинів та їх ознаки; формувати правильний опис кіберподії. ***Рекомендовані джерела:*** 1-6; 9-10; 24	Лекція 1	4*	Лекція-візуалізація
	Практичне заняття 1		Опрацювання ситуаційних завдань; кейси, усне опитування, тестування Kahoot , навчальна дискусія
	Практичне заняття 2		Виконання завдань за вказівками. Експрес опитування
Тема 2. **Методи та інструменти цифрової криміналістики** ***Знати***: життєвий цикл цифрових доказів; методи форензичного аналізу ПК, мобільних пристроїв і серверів; форензік як інструмент фінансового розслідування діяльності підприємства; формат і зміст форензичного звіту. ***Вміти***: використовувати методи виявлення, фіксації та збирання цифрових доказів у мережевому та локальному середовищах; застосовувати знання для проведення комп'ютерно-технічної експертизи, цифрової криміналістики та відтворення подій кіберінциденту; проводити вилучення, фіксацію та збереження цифрових доказів; застосовувати утиліти Autopsy, FTK Imager, Volatility, Sleuth Kit; документувати результати форензичного дослідження. ***Рекомендовані джерела:*** 1-6; 11; 13; 18-20.	Лекція 2	6*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3		Мозковий штурм; інтерактивні завдання; опитування (відкриті питання)
	Практичне заняття 4		Усне опитування, тематична дискусія: презентація матеріалів
Тема 3. **Виявлення та розслідування кіберінцидентів** ***Знати***: принципи побудови систем IR; алгоритм реагування на кіберінциденти; методи аналізу журналів подій; процедури реагування на інциденти. ***Вміти***: використовувати професійні інструменти (Splunk, Wazuh, Suricata, Snort); створювати сценарії реагування на інциденти; аналізувати трафік і журнали подій.. ***Рекомендовані джерела***: 1; 7-9; 12	Лекція 3	6*	Лекція-візуалізація
	Практичне заняття 5		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей
	Практичне заняття 6		Усне опитування, тестування у Kahoot , навчальна дискусія
Тема 4. **Електронні докази у кримінальному провадженні** ***Знати***: поняття електронних (цифрових) доказів у кримінальному провадженні та їх види; способи збирання електронних доказів ***Вміти***: проводити статичний аналіз файлів; проводити динамічний аналіз шкідливого ПЗ; аналізувати поведінки та мережевої активності; проводити фіксацію й документування результатів аналізу. ***Рекомендовані джерела:*** 1; 13-22	Лекція 4	6* (+15 МК1)	Лекція-візуалізація
	Практичне заняття 7		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей
	Практичне заняття 8		Усне опитування. Проведення контролю знань №1
Розділ 2. Практичні аспекти протидії кібеззлочинності			

Тема 5. **Аналіз шкідливого програмного забезпечення** ***Знати***: основні типи шкідливого ПЗ та механізми їх роботи; методи аналізу у «пісочниці» ознаки інфікування та методи приховування.***Вміти***: розробляти основні положення політики, визначати бюджет і KPI ІБ. ***Рекомендовані джерела:*** 1; 5; 14-20	Лекція 5	3*	Лекція-візуалізація
	Практичне заняття 9		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей.
	Практичне заняття 10		Усне опитування, практичне опрацювання за матеріалами лекції
Тема6. **Протидія технікам злому та обходу захисту** ***Знати:*** основні атаки на мережеву інфраструктуру; атаки на вебдодатки та засоби захисту; особливості експлуатації вразливостей (Exploitation); інструменти соціальної інженерії, які використовує кіберзлочинець: методи попередження та мінімізації наслідків атак. ***Вміти:*** визначати вразливості в конфігураціях систем; обирати контрзаходи проти різних типів атак; використовувати методи попередження та мінімізації наслідків атак; проводити етичне тестування на проникнення. ***Рекомендовані джерела:*** 1; 22-30	Лекція 6	3*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 11		Доповідь з презентацією за тематикою теми та її обговорення.
	Практичне заняття 12		Усне опитування, навчальна дискусія, ситуаційні завдання
Тема 7. **Моніторинг кіберзагроз та OSINT-розвідка** ***Знати***: методологію відкритої розвідки (OSINT); інструменти збору інформації про кіберзагрози.; особливості аналізу цифрового сліду; конфігурації профілю кіберзагрози; особливості прогнозування та моделювання поведінки зловмисника. ***Вміти***: використовувати джерела інформації про загрози (Threat Intelligence); працювати з Maltego, Shodan, SpiderFoot; аналізувати цифрові профілі кібезлочинців ***Рекомендовані джерела:*** 1; 11; 27-33	Лекція 7	6*	Лекція-візуалізація
	Практичне заняття 13		Ситуаційні завдання
	Практичне заняття 14		Усне опитування, презентації та доповіді, обговорення.
Тема 8. **Моделювання кіберзагроз і аналіз вразливостей** ***Знати***: стандарти оцінювання вразливостей; моделі загроз STRIDE, MITRE ATT&CK; техніки моделювання ризиків; побудова карти кіберзагроз; пріоритизація вразливостей. ***Вміти***: моделювати атаки з використанням ATT&CK; визначати критичність вразливостей. ***Рекомендовані джерела:*** 1; 6; 13-20	Лекція 8	3*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 15		Усне опитування, презентації. Доповіді. Обговорення за результатами доповідей.
	Практичне заняття 16		Усне опитування, навчальна дискусія, ситуаційні завдання.
Тема 9. **Протидія кібертероризму, кіберзлочинності та гібридним проявам кібервійн в Україні** ***Знати***: ключові визначення та ознаки кібертероризму, його відмінність від інших форм кіберзлочинності та кіберзагроз; типові інструменти та тактики кібертерористичних атак, включно з DDoS, порушенням роботи критичної інфраструктури, шкідливим ПЗ, шифрувальниками, деструктивними програмами; структуру та особливості кіберзлочинних мереж, зокрема їх	Лекція 9	3* (+15 МК2)	Лекція-візуалізація Експрес-опитування.
	Практичне заняття 17		Навчальна дискусія, опрацювання опанованого матеріалу та усне опитування, тестування у Kahoot
	Практичне		Доповіді з презентацією.

взаємодію з державними або квазідержавними акторами; форми та елементи гібридної кібервійни, включно з інформаційно-психологічними операціями, деструктивними атаками на урядові та цивільні об'єкти, атакою на енергетичний сектор, транспорт, зв'язок; технологічні підходи до запобігання та попередження кіберінцидентів, їх ескалації та впливу на національну безпеку. ***Вміти***: аналізувати та ідентифікувати ознаки кібертерористичних або гібридних атак, розмежовувати їх від звичайних кіберзлочинних подій; оцінювати рівень ризику та потенційні наслідки кібератак для об'єктів критичної інфраструктури, державних органів та приватного сектору; застосовувати методи виявлення та реагування на кібертерористичні загрози, зокрема аналіз логів, мережевого трафіку, поведінкових індикаторів; розробляти рекомендації з підвищення кіберстійкості організацій, включно з технічними, організаційними та інформаційно-комунікаційними заходами; формувати аналітичні висновки щодо інцидентів, формулювати пропозиції з мінімізації загроз, протидії інформаційно-психологічним впливам і посилення спроможностей кіберзахисту ***Рекомендовані джерела:***1; 34-39.	заняття 18		Проведення контролю знань №2
Залік	Проведення заліку	40*	
Самостійна робота		*	Завдання із переліку запропонованих проблемних питань для дослідження за тематикою наукових інтересів здобувача освіти у межах дисципліни

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕНН ДИСЦИПЛІНИ

Комп'ютери с програмним забезпеченням для виконання практичних робіт: комп'ютери Asus, комп'ютерний клас для проведення занять
Спеціалізована лабораторія: «Security operation center» кафедри управління кібербезпекою та захистом інформації.
Мультимедійний проєктор, мультимедійна система Acer X113 DLP
Google Workspace for Education

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Навчально-методичний комплекс з дисципліни «Методи та засоби протидії кіберзлочинності» для студентів спеціальності F5 «Кібербезпека та захист інформації» та студентів інших спеціальностей. Google Workspace for Education - https://classroom.google.com/
2. Lehominova S., Zaporozhchenko M., Kapeliushna T., Shchavinskyi Yu., Muzhanova T. Method for assessing the risk of user compromise based on individual security profile. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2026. Vol. 16 No. 1. C. 130-137.
3. Капелюшна, Т., Мужанова, Т., Берестяна, Т., Голобородько, С., & Примаченко, Д. (2025). Механізм управління доступом до інформаційних ресурсів на підприємстві. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 205–219. https://doi.org/10.28925/2663-4023.2025.27.743
4. Легомінова, С., Капелюшна, Т., Щавінський, Ю., Запорожченко, М., & Будзинський, О. (2025). Концепція автоматизованого реагування на загрози в корпоративних базах даних у режимі реального часу. «Кібербезпека: освіта, наука, техніка». 1(29), С. 676–686. https://doi.org/10.28925/2663-4023.2025.29.927
5. Капелюшна Т.В. Легомінова С.В., Мужанова Т.М., Тищенко В.С. Регуляторне поле формування політики управління інформаційною безпекою організації. Кібербезпека: освіта, наука, техніка. 2024, 2 (26), pp. 235-245. DOI 10.28925/2663-4023.2024.26.693
6. Капелюшна Т.В. Легомінова С.В., Тищенко В.С., Недодай М.Г., Дьячук О.С. Штучний інтелект та соціальні мережі: підходи до виявлення фейкової інформації. Телекомунікаційні та інформаційні технології. 2024, 4 (85), pp. 83-89. DOI 10.31673/2412-4338.2024.044748
7. Аніщук В.В., Зициг С.Г. ПРОБЛЕМА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ:ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ. Проблема протидії кіберзлочинності: порівняльно-правовий аналізТом 3 № 83 (2024): Науковий вісник Ужгородського національного університету. Серія: Право. https://doi.org/10.24144/2307-3322.2024.83.3.2
8. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. Науковий вісник Ужгородського університету: серія: Право / голов. ред. Ю. М. Бисага. Ужгород: Видавничий дім «Гельветика», 2023. Т. 2. Вип. 75. С. 83-87. Бібліогр.: с. 86-87.
9. Діброва Т. А. Кіберзлочинність та кібершахрайство в умовах воєнного стану. Юридичний науковий електронний журнал. 2022. № 11. С. 546-549.
10. Лавник А. М. Державна політика протидії кіберзлочинності в умовах інформаційної війни рф проти України. Національний авіаційний університет. 2023. 55 с

11. Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі : наук.-практ. посібник : електрон. наук. вид. / [Шепітько В. Ю., Авдєєва Г. К., Коновалова В. О. та ін.] ; за ред. В. Ю. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2023. – 116 с. https://ivpz.kh.ua/wp-content/uploads/2024/02/%D0%9F%D0%BE%D1%81%D1%96%D0%B1_%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B0_2023_%D0%9D%D0%94%D0%86-%D0%92%D0%9F%D0%97_%D0%9F%D0%921_compressed.pdfПЕРЕДЕРІЙ, О.С. (2025). Заходи забезпечення прав дитини як учасника цифрових відносин в аспекті протидії кіберзлочинності та втягненню в протиправну діяльністьmeasures to protect the rights of the child as participant of digital relations in the aspect of combating cybercrime and involvement in illegal activities. Вісник Кримінологічної асоціації України. 35. 376-384. 10.32631/vca.2025.2.31.
12. Передерій, О.С & Кулачок-Тітова, Л.В. (2025). Організаційно-правові заходи забезпечення безпеки цифрових послуг в аспекті протидії кіберзлочинності в Україні. Вісник Кримінологічної асоціації України. 34. 570-578. 10.32631/vca.2025.1.44.
13. Корзун, Світлана. (2024). Теоретико-методологічна конструкція державної кримінально-правової політики протидії кіберзлочинності. Економіка, управління та адміністрування. 145-158. 10.26642/ema-2024-4(110)-145-158.
14. Рульов І.М. Співвідношення кібертероризму та кіберзлочину. Юридичний вісник. Одеса: Гельветика, 2021. № 3. С. 178–185.
15. Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни. Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023.
16. Легомінова С., Якименко Ю.,Мужанова Т., Капелюшна Т. Вплив управління інцидентами на функціонування системи управління інформаційною безпекою організації. *Телекомунікаційні та інформаційні технології.* 1 (25). С. 75-81. https://doi.org/10.31673/2412-4338.2025.014011
17. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М.Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак,О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2024. – 370 с. https://profbook.com.ua/index.php?route=product/product/download&product_id=8999&download_id=2047&srsltid=AfmBOoq2vv_XN2sGZh3ZihX1w9dUSltDZnH3ijsLeJy5HV20qssemMBM
18. Чубаєвський, В. (2022). Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*, (43). https://doi.org/10.32782/2524-0072/2022-43-49
19. Ткаченко О.А, Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, №1. С. 75-86.
20. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
21. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
22. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерноінтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
23. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf
24. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
25. Ткаченко О.А, Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, №1. С. 75-86.
26. Захистіть корпоративне середовище від кіберзагроз. https://www.eset.com/ua/business/enterprise/?srsltid=AfmBOorJYq7EoBgxAVPZhJSQ_i9smWDAEoXPzWak88lEoghGCf6n_TN1#threat-intelligence
27. Безпека Ваших пристроїв: 7https://dovidka.info/kiberbezpeka/
28. Принципи запровадження кіберкультури: https://moz.gov.ua/uk/principi-zaprovadzhennya-kiberkulturi
29. Куперштайн Л., Малиновський В, Каплун В. КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ / КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ: https://www.researchgate.net/publication/379257182_CYBER_SECURITY_OF_MOBILE_DEVICES_AND_INTERNET_OF_THINGS_KIBERBEZPEKA_MOBILNIH_PRISTROIV_TA_INTERNETU_RECEJ
30. Phishing Explained In 6 Minutes | What Is A Phishing Attack? URL: https://youtu.be/XBkzBrXlle0
31. Звіт 2025 Cyber Threat Report https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report
32. Савчук С.О. ДЕРЖАВНА ПОЛІТИКА ПРОТИДІЇ КАБЕРЗЛОЧИННОСТІ. https://hackyourmom.com/kibervijna/fishyngovi-kampaniyi-apt29-ta-apt35-analiz-klyuchovyh-atak/
33. Офіційний сайт COREWIN. Найбільші та найвідоміші кібератаки в історії https://corewin.ua/blog/biggest-cyber-attacks-in-history/
34. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.
35. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії. Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Випуск 40, с.Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 40, p. 186–191.
36. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с.
37. Schmid Johann. Der Archetypus hybrider Kriegführung. Hybride Kriegführung vs. Militärisch zentrierte Kriegführung. In: Österreichische Militärische Zeitschrift (ÖMZ), 2020. Heft 5/2020, P. 570–579.
38. Бєляков К.І. Інформація в праві: теорія і практика. Монографія. – Київ: Видавництво "КВІЦ", 2006. – 116 с.; 1 іл. https://ippi.org.ua/sites/default/files/informaciya_v_prave.pdf
39. Курбан О. (2015). Theory of information warfare: basic framework, methodology and conceptual apparatus. ScienceRise. 11. 95. 10.15587/2313-8416.2015.53940

ПОЛІТИКА КУРСУ

- 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 зазначений 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

Форми контролю	Види навчальної роботи	* Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на лекціях,*** *у т.ч.:*	
	• ведення конспекту	за кожну лекцію 0,5 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	Робота на практичних заняттях*, у т.ч.:*	
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді)	за кожну презентацію максимум 4 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 2 бали
РУБІЖНЕ ОЦІНЮВАННЯ (контроль знань)	Контроль знань № 1	за кожне правильно виконане завдання максимальна оцінка – 30 балів
	Контроль знань № 2	за кожне правильно виконане завдання максимальна оцінка – 30 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Згідно рішення кафедри
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у формі тестування	40 балів

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	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені	Добре / Зараховано (В)

	практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	дисципліни	
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 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 заліку.	**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