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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ШТУЧНИЙ ІНТЕЛЕКТ В КІБЕРБЕЗПЕЦІ»

Лектор курсу			**Запорожченко Михайло Михайлович,** доцент кафедри управління кібербезпекою та захистом інформації		**Контактна інформація лектора (e-mail), сторінка курсу в Google Classroom**	**e-mail:** m.zaporozhchenko@duikt.edu.ua; **сторінка курсу в Google Classroom –** https://classroom.google.com/	
Галузь знань			F «Інформаційні технології»		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			F5 «Кібербезпека та захист інформації»		**Семестр**	7	
Освітня програма			«Управління інформаційною та кібернетичною безпекою»		**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

Мета курсу:	формування у здобувачів знань і практичних навичок застосування методів штучного інтелекту для розв’язання задач кібербезпеки та захисту інформації.

Програмні компетенції

Загальні компетентності (ЗК)	Спеціальні (фахові, предментні) компетентності (СК)
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 використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

Програмні результати навчання (РН)

РН5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
МОДУЛЬ 1 «ОСНОВИ ШТУЧНОГО ІНТЕЛЕКТУ ТА АНАЛІЗУ ДАНИХ У КІБЕРБЕЗПЕЦІ»			
Тема 1. Основи штучного інтелекту в кібербезпеці ***Знати***: основні поняття та визначення у сфері штучного інтелекту, машинного навчання та глибокого навчання; відмінності між AI, ML, DL та генеративним штучним інтелектом; основні типи задач машинного навчання; особливості застосування штучного інтелекту для забезпечення кібербезпеки; типові сценарії використання AI у системах захисту інформації; переваги, обмеження та ризики використання AI у кібербезпеці. ***Вміти***: визначати доцільність застосування методів штучного інтелекту для розв'язання задач кібербезпеки; класифікувати задачі кібербезпеки за типом задачі машинного навчання; обирати відповідний підхід AI залежно від характеру даних і поставленої задачі; оцінювати переваги та обмеження застосування AI у конкретній ситуації. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 1 2 год	5	Лекція-візуалізація
	Практичне заняття 1 2 год		Практична робота: Визначення задач кібербезпеки, для яких доцільне застосування штучного інтелекту. Аналіз сценаріїв використання AI для виявлення загроз, аналізу подій безпеки та підтримки прийняття рішень.
	Самостійна робота		Огляд сучасних напрямів застосування штучного інтелекту в кібербезпеці; порівняння AI, ML, DL та генеративного AI; аналіз прикладів використання AI у системах моніторингу та захисту інформації.
Тема 2. Дані та ознаки для задач кібербезпеки ***Знати***: поняття набору даних, ознаки, цільової змінної та вибірки; основні типи даних, що використовуються в кібербезпеці; джерела даних для машинного навчання; принципи підготовки та очищення даних; проблеми пропущених, зашумлених і незбалансованих даних; поняття feature engineering та feature selection. ***Вміти***: визначати джерела даних для задач кібербезпеки; формувати набір ознак для задач класифікації та виявлення аномалій; виконувати базову підготовку даних; визначати ознаки, що мають інформаційну цінність для задачі; виявляти проблеми якості та дисбалансу даних. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 2 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 2 2 год		Практична робота: Підготовка набору даних для задачі кібербезпеки. Аналіз ознак мережевого трафіку, подій журналів або характеристик користувацької активності. Виявлення пропущених значень, дублювання та дисбалансу класів.
	Самостійна робота		Дослідження наборів даних для кібербезпеки; аналіз структури журналів подій; дослідження методів відбору та перетворення ознак; підготовка переліку ознак для конкретної задачі виявлення кіберзагроз.

Тема 3. Машинне навчання для класифікації кіберзагроз ***Знати***: поняття навчання з учителем; принципи задач класифікації; основні алгоритми машинного навчання для класифікації; поняття навчальної, валідаційної та тестової вибірок; перенавчання та недонавчання; основні метрики оцінювання моделей класифікації. ***Вміти***: формулювати задачу класифікації у сфері кібербезпеки; готувати дані для навчання класифікатора; застосовувати базові алгоритми машинного навчання; оцінювати якість моделі за показниками accuracy, precision, recall, F1-score та матрицею помилок; порівнювати результати різних моделей. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 3 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 3 2 год		Практична робота: Побудова та оцінювання моделі класифікації для виявлення кіберзагроз. Порівняння результатів роботи моделей за основними метриками.
	Самостійна робота		Дослідження алгоритмів дерева рішень, випадкового лісу, логістичної регресії та методів опорних векторів; аналіз проблеми перенавчання; порівняння метрик оцінювання моделей для задач кібербезпеки.
МОДУЛЬ 2 «МЕТОДИ МАШИННОГО ТА ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ»			
Тема 4. Виявлення аномалій та невідомих загроз ***Знати***: поняття аномалії та відхилення від нормальної поведінки; принципи навчання без учителя; основні методи кластеризації та виявлення аномалій; особливості застосування методів unsupervised learning у кібербезпеці; поняття baseline поведінки та його використання для виявлення підозрілої активності. ***Вміти***: формулювати задачу виявлення аномалій; визначати нормальну та аномальну поведінку за набором ознак; застосовувати методи кластеризації та виявлення аномалій; інтерпретувати результати роботи алгоритмів; оцінювати доцільність використання unsupervised learning для виявлення невідомих загроз. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 4 2 год	5	Лекція-візуалізація
	Практичне заняття 4 2 год		Практична робота: Виявлення аномальної активності користувачів або мережевого трафіку методами машинного навчання без учителя. Формування профілю нормальної поведінки та визначення відхилень.
	Самостійна робота		Дослідження методів кластеризації; аналіз алгоритмів виявлення аномалій; дослідження застосування unsupervised learning у системах IDS/IPS та SIEM; аналіз проблеми хибних спрацювань.
Тема 5. Глибоке навчання у системах кібербезпеки ***Знати***: основні принципи глибокого навчання; архітектуру та призначення нейронних мереж; поняття шару, нейрона, функції активації та вагових коефіцієнтів; особливості застосування CNN, RNN та інших архітектур для задач аналізу даних кібербезпеки; переваги та обмеження deep learning. ***Вміти***: визначати доцільність використання нейронних мереж для задач кібербезпеки; формувати постановку задачі для нейронної	Лекція 5 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5 2 год		Практична робота: Побудова та оцінювання простої нейронної мережі для задачі класифікації кіберзагроз. Аналіз результатів навчання та помилок моделі.

мережі; аналізувати результати навчання моделі; визначати ознаки перенавчання; порівнювати класичні алгоритми ML та методи DL для конкретної задачі. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Самостійна робота		Дослідження архітектур CNN, RNN та трансформерів; аналіз застосування глибокого навчання для аналізу мережевого трафіку, шкідливого програмного забезпечення та журналів подій.
Тема 6. Обробка текстових даних та виявлення соціоінженерних загроз ***Знати***: основи обробки природної мови; поняття токенізації, векторного представлення тексту та embeddings; принципи застосування NLP у кібербезпеці; методи аналізу електронних листів, повідомлень та інших текстових даних; можливості AI для виявлення ознак фішингу та соціальної інженерії. ***Вміти***: визначати текстові ознаки, що можуть використовуватися для виявлення соціоінженерних загроз; здійснювати базову підготовку текстових даних; аналізувати результати класифікації текстів; оцінювати можливості та обмеження NLP-моделей у задачах інформаційної безпеки. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 6 2 год	5	Лекція-візуалізація, експрес-опитування
	Практичне заняття 6 2 год		Практична робота: Аналіз текстових повідомлень для виявлення ознак фішингової та соціоінженерної комунікації. Формування ознак тексту та оцінювання результатів класифікації.
	Самостійна робота		Дослідження застосування NLP у кібербезпеці; аналіз методів виявлення фішингових повідомлень; дослідження можливостей мовних моделей для аналізу текстових даних та кіберзагроз.
МОДУЛЬ 3 «ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ, БЕЗПЕКА AI-СИСТЕМ ТА ЇХ ЗАСТОСУВАННЯ»			
Тема 7. Генеративний штучний інтелект та великі мовні моделі в кібербезпеці ***Знати***: поняття генеративного штучного інтелекту, великих мовних моделей та трансформерів; принципи функціонування сучасних мовних моделей на концептуальному рівні; основні напрями використання генеративного AI у кібербезпеці; можливості AI для аналізу журналів, документації, інцидентів та підтримки діяльності фахівця з кібербезпеки; поняття hallucination та інші обмеження генеративних моделей. ***Вміти:*** формулювати задачі для генеративних AI-систем у професійній діяльності; оцінювати якість та достовірність отриманих результатів; використовувати AI для структурування та аналізу інформації про події безпеки; критично оцінювати результати роботи мовних моделей; визначати випадки, коли рішення AI потребує перевірки фахівцем. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 7 2 год	5	Лекція-візуалізація
	Практичне заняття 7 2 год		Практична робота: Використання генеративного AI для аналізу подій інформаційної безпеки, структурування журналів та формування аналітичних висновків. Перевірка достовірності результатів AI.
	Самостійна робота		Дослідження архітектури трансформерів та принципів роботи LLM; аналіз можливостей генеративного AI для SOC; дослідження проблеми hallucination та способів верифікації результатів AI.

Тема 8. Безпека систем штучного інтелекту та атаки на моделі ***Знати***: основні загрози для систем штучного інтелекту; поняття adversarial machine learning; основні типи атак на моделі машинного навчання; ризики отруєння даних, маніпулювання вхідними даними та витоку інформації; проблеми конфіденційності, цілісності та достовірності AI-моделей; принципи захисту AI-систем. ***Вміти***: ідентифікувати основні загрози для AI-систем; аналізувати ризики використання моделей машинного навчання в інформаційних системах; оцінювати стійкість AI-рішень до маніпуляцій; визначати необхідні заходи захисту даних, моделей та результатів їх роботи; формувати базові рекомендації щодо безпечного використання AI у кібербезпеці. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 8 2 год	5	Лекція-візуалізація
	Практичне заняття 8 2 год		Практична робота: Аналіз загроз та вразливостей систем штучного інтелекту. Побудова моделі загроз для AI-системи та визначення заходів її захисту.
	Самостійна робота		Дослідження основних типів adversarial attacks; аналіз ризиків poisoning та evasion; дослідження методів захисту моделей машинного навчання; аналіз безпеки даних, що використовуються для навчання AI.
Тема 9. Штучний інтелект у системах моніторингу та реагування на кіберінциденти ***Знати***: роль штучного інтелекту в SOC; принципи використання AI для аналізу подій інформаційної безпеки; можливості AI у SIEM, IDS/IPS та системах виявлення аномалій; поняття автоматизованого аналізу та пріоритизації подій; переваги та обмеження автоматизації процесів реагування на кіберінциденти; принципи відповідального використання AI під час прийняття рішень у сфері кібербезпеки. ***Вміти***: визначати задачі SOC, які можуть бути автоматизовані за допомогою AI; аналізувати та класифікувати події інформаційної безпеки; використовувати результати роботи AI для підтримки прийняття рішень; оцінювати ризики автоматизованих рішень; формувати концепцію AI-компонента системи моніторингу та реагування на кіберінциденти. ***Формування компетенцій:*** ІК, ЗК1, ЗК2, СК2. ***Результати навчання:*** РН5, РН10. ***Рекомендовані джерела:*** 1-22	Лекція 9 2 год	5	Лекція-візуалізація
	Практичне заняття 9 2 год		Практична робота: Розроблення концепту AI-компонента системи кібербезпеки. Аналіз подій безпеки, визначення пріоритетності інцидентів та формування рекомендацій щодо реагування.
	Самостійна робота		Дослідження практик використання AI у SOC; аналіз застосування AI у SIEM та системах виявлення атак; розроблення концепції використання AI для конкретної задачі кібербезпеки; аналіз ризиків та обмежень автоматизації прийняття рішень.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Навчальна лабораторія «Центр управління інформаційною та кібернетичною безпекою» («Security Operation Center»).
- Перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій та слайдів до лекцій через систему Google Classroom для підготовки до практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Yurii Shchavinsky, Tetiana Muzhanova, Yuriy Yakymenko, Mykhailo Zaporozhchenko. Application of artificial intelligence for improving situational training of cybersecurity specialists. Information Technologies and Learning Tools. 2023. Vol. 97, № 5. P. 215-226. URL: https://doi.org/10.33407/itlt.v97i5.5424
2. Svitlana Lehominova, Yurii Shchavinsky, Tetiana Muzhanova, Dmytro Rabchun, Mykhailo Zaporozhchenko. Application of sentiment analysis to prevent cyberattacks on objects of critical information infrastructure. International Journal of Computing. 2023. Vol. 22, № 4. P. 534-540. URL: https://doi.org/10.47839/ijc.22.4.3362
3. 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
4. Будзинський О., Щавінський Ю., Мужанова Т., Якименко Ю., Примаченко Д. Методика інтелектуальної оцінки ризиків інформаційної безпеки корпоративних баз даних. Кібербезпека: освіта, наука, техніка. 2026. Том 1, № 33. P. 399–413. URL: https://doi.org/10.28925/2663-4023.2026.33.1221
5. Svitlana Lehominova, Tetiana Kapeliushna, Yurii Shchavinskyi, Mykhailo Zaporozhchenko, Oleksandr Budzynskyi. Concept of automated response to threats in corporate databases in real-time mode. Кібербезпека: освіта, наука, техніка. 2025. Том 1, № 29. С. 676-686. URL: https://doi.org/10.28925/2663-4023.2025.29.927
6. Zhang A., Lipton Z. C., Li M., Smola A. J. Dive into Deep Learning. Cambridge : Cambridge University Press, 2023. 574 p. URL: https://d2l.ai/
7. Molnar C. Interpretable Machine Learning : A Guide for Making Black Box Models Explainable. 3rd ed., 2025. URL: https://christophm.github.io/interpretable-ml-book/
8. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. Sebastopol: O'Reilly Media, 2018. 384 p. URL: https://mlsec.net/
9. Sipola T., Kokkonen T., Karjalainen M., eds. Artificial Intelligence and Cybersecurity : Theory and Applications. Cham : Springer, 2023. 301 p. DOI: 10.1007/978-3-031-15030-2. URL: https://link.springer.com/book/10.1007/978-3-031-15030-2
10. Sewak M., Sahay S. K., Rathore H. Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review. 2022. URL: https://arxiv.org/abs/2206.02733
11. Xi B. Adversarial Machine Learning for Cybersecurity and Computer Vision: Current Developments and Challenges. 2021. URL: https://doi.org/10.48550/arXiv.2107.02894
12. Roy P., Chandrasekaran J., Lanus E., Freeman L., Werner J. A Survey of Data Security: Practices from Cybersecurity and Challenges of Machine Learning. 2023. URL: https://arxiv.org/abs/2310.04513
13. Зоря І. С., Марущак А. В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. Вінниця : Вінницький національний технічний університет, 2024. URL: https://ir.lib.vntu.edu.ua/handle/123456789/42057
14. Притула А. В., Куперштейн Л. М. Застосування штучного інтелекту для тестування на проникнення. Вінниця : Вінницький національний технічний університет, 2024. URL: https://ir.lib.vntu.edu.ua/handle/123456789/41901
15. Василинич М. В., Василинич А. В., Притула М. О. Роль штучного інтелекту в інформаційній безпеці України. Вінниця : Вінницький національний технічний університет, 2025. URL: https://ir.lib.vntu.edu.ua/handle/123456789/47934
16. Войтович О. П., Пилявець І. Ю., Радченко Є. В. Використання штучного інтелекту в аудиті інформаційної безпеки. Вінниця : Вінницький національний технічний університет, 2025. URL: https://ir.lib.vntu.edu.ua/handle/123456789/47915
17. Главчев М. І., Главчев Д. М., Панченко В. І. Балансування навантаження системи штучного інтелекту для запобігання DDoS-атакам. Системи обробки інформації. 2025. № 4(183). С. 7–14. DOI: 10.30748/soi.2025.183.01. URL: https://journal-hnups.com.ua/index.php/soi/article/view/2493
18. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence Cybersecurity Challenges. Heraklion : ENISA, 2020. URL: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
19. Повний текст відкритий. Документ містить систематизацію загроз AI та проблем безпеки протягом життєвого циклу AI-систем.
20. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence and Cybersecurity Research. Heraklion : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research
21. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : NIST, 2023. 43 p. NIST AI 100-1. DOI: 10.6028/NIST.AI.100-1. URL: https://doi.org/10.6028/NIST.AI.100-1
22. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Gaithersburg : NIST, 2024. 48 p. NIST AI 600-1. URL: https://doi.org/10.6028/NIST.AI.600-1

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 40 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 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «ОСНОВИ ШТУЧНОГО ІНТЕЛЕКТУ ТА АНАЛІЗУ ДАНИХ У КІБЕРБЕЗПЕЦІ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «МЕТОДИ МАШИННОГО ТА ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ»	максимальна оцінка – 15 балів
	Модульний контроль № 3 «ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ, БЕЗПЕКА AI-СИСТЕМ ТА ЇХ ЗАСТОСУВАННЯ»	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від Заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в заліковій відомості*
90	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій	**Високий**	Відмінно /

	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.	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.	Зараховано (A)
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)
3 5	Студент може відтворити окремі фрагменти з курсу.	**Низький**	Незадовільно з

	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.	Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	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