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

СИЛАБУС НАВЧАЛЬНОЇ КОМПОНЕНТИ
«Системи управління інформаційною безпекою»

Лектор курсу			**Легомінова Світлана Володимирівна,** доктор економічних наук, професор. завідувач кафедри Управління кібербезпекою та захистом інформації		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** s.legominova@duikt.edu.ua; **сторінка курсу в Classroom –** https://classroom.google.com/c/ODQ1NjMxNTAxOTIz?cjc=ms7tz2jp	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**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	18	–	36	–	36

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Дисципліни професійної підготовки бакалаврського рівня.
Освітні компоненти для яких є базовою	Управління проєктами. Переддипломна практика. Кваліфікаційна робота.

Мета курсу:	Формування у здобувачів освіти теоретичних знань та практичних навичок щодо побудови, впровадження, функціонування й удосконалення систем управління інформаційною безпекою на основі системного підходу, сучасних методів та засобів, а також з урахуванням вимог міжнародних і національних стандартів у сфері інформаційної та кібербезпеки.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях.	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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики

Програмні результати навчання (ПРН)			
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізикоматематичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема,опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Основні поняття та принципи створення системи управління інформаційною безпекою **Знати:** основні терміни і визначення управління інформаційною безпекою (ІБ), напрямки організаційної і управлінської роботи у сфері ІБ, методологію організаційного забезпечення, проблеми управління ІБ, закон єдності аналізу і синтезу в процесах управління, реалізація системного підходу в дослідженні СУІБ, методи досліджень СУІБ, системні рішення питань вимірювання ефективності СУІБ, методологію побудови ефективної СУІБ. **Вміти:** проводити дослідження та використовувати методологію організаційного забезпечення в вирішенні проблем управління ІБ і побудови ефективної СУІБ. **Формування компетентностей:** К31, КФ2, КФ4. **Результати навчання:** РН5, РН8, РН9. **Рекомендовані джерела:** 1–4, 8–10, 15–17.			
Мета вивчення дисципліни. Основні терміни і визначення.	Лекція 1 2 год		Лекція-візуалізація
Аналіз стану проблем УІБ	Пз 1 2 год	3 бали	Практичні заняття проводяться на основі реалістичних кейсів з акцентом на сучасні методи досліджень для вироблення рішень у сфері управління інформаційною безпекою.
Аналіз концептуальної схеми забезпечення інформаційної безпеки	Пз 2 2 год	3 бали	
Мета, завдання, передумови та напрямки організаційної і управлінської роботи у сфері інформаційної безпеки	Лекція 2 2 год		Лекція-візуалізація
Аналіз методичних інструментів в дослідженнях СУІБ	Пз 3 2 год	3 бали	Практичні заняття проводяться на основі реалістичних кейсів з акцентом на методи аналізу і синтезу для побудови ефективних СУІБ.
Аналіз та синтез як методи в процесах управління СУІБ	Пз 4 2 год	3 бали	
Загальна методологія організаційного забезпечення інформаційної безпеки	Лекція 3 2 год		Лекція-візуалізація
Вимірювання ефективності СУІБ - на прикладах	Пз 5 2 год	3 бали	Практичні заняття проводяться на основі реалістичних кейсів з акцентом на методи дослідження та групові обговорення для вироблення рішень у сфері управління інформаційною безпекою.
Методологічні підходи до дослідження СУІБ	Пз 6 2 год	3 бали	
Тема 1. Основні поняття та принципи створення системи	Самостійна	6 балів	**Питання для самостійного опрацювання:** Основні напрямки

управління інформаційною безпекою.	робота 12 год		розвитку менеджменту в сфері ІБ. Проблеми управління ІБ. Комплексні проблеми в інформаційній сфері України і методи їх запобігання та ліквідації. Десять кроків до надійної системи ІБ. Загальна методологія організаційного забезпечення ІБ. Особливості нормативно-правового забезпечення СУІБ. Методологія організаційного забезпечення ІБ на рівні великих постачальників інформаційних систем. Об'єктивні фактори, як передумови становлення інформаційного права України. Організаційне забезпечення ІБ на рівні окремих великих компаній. Методи досліджень СУІБ. Дослідження як функція управління. Досвід створення СУІБ. Управління активами в СУІБ. Документаційне забезпечення СУІБ.
Тема 2. Концепції та моделі системи управління інформаційною безпекою. **Знати:** Модель "Плануй-Виконуй-Перевіряй-Дій", використання системного підходу до управління ІБ, порядок створення комплексної системи управління інформаційною безпекою (процесний підхід), вимоги міжнародних стандартів з питань управління ІБ, методику формування нормативних (розпорядчих та методичних) документів в процесі впровадження та функціонування СУІБ, алгоритм впровадження СУІБ за методикою ІТ-Груншутца, етапи розробки та впровадження СУІБ, концепцію і напрями ІБ, документаційне забезпечення СУІБ та управління активами. **Вміти:** розробляти концепції, положення та функціональні обов'язки посадових осіб для експлуатації СУІБ; на основі аналізу результатів досліджень розробляти рекомендації щодо удосконалення СУІБ. **Формування компетентностей:** КЗ1, КФ2, КФ4, КФ6. **Результати навчання:** РН8, РН9, РН11. **Рекомендовані джерела:** 1, 2, 5, 6, 11–14.			
Використання метрик управління інформаційною безпекою	Лекція 4 2 год		Лекція-візуалізація
Реалізація процесного підходу до побудови СУІБ	Пз 7 2 год	3 бали	Практичні заняття проводяться у формі роботи з практичними кейсами щодо аналізу вимог міжнародних і національних стандартів, моделювання процесного та системного підходів для побудови СУІБ з акцентом на застосування дослідницьких і практико-орієнтованих методів.
Реалізація системного підходу до побудови СУІБ	Пз 8 2 год	3 бали	
Міжнародні стандарти з питань управління інформаційною безпекою	Лекція 5 2 год		Лекція-візуалізація
Вивчення вимог стандартів серії ДСТУ ISO до побудови СУІБ	Пз 9 2 год	3 бали	Практичні заняття проводяться у формі роботи з кейсами аналізу вимог міжнародних і національних стандартів, відпрацювання процедур аудиту та розробки нормативних документів СУІБ з використанням наукових методів досліджень.
Організація сертифікаційного аудиту та наглядових аудитів	Пз 10 2 год	3 бали	
Методика формування нормативних, розпорядчих та методичних документів в процесі впровадження та функціонування СУІБ	Лекція 6 2 год		Лекція-візуалізація

Розробка документів функціонування СУІБ	Пз 11 2 год	3 бали	Практичні заняття проводяться у формі роботи з кейсами розробки нормативних документів СУІБ з акцентом на застосування практико-орієнтованих методів досліджень.
Проміжний контроль	Пз 12 2 год	3 бали	
Тема 2. Концепції та моделі системи управління інформаційною безпекою	Самостійна робота 12 год	6 балів	**Питання для самостійного опрацювання:** Моделювання СУІБ. Принципи системного і процесного підходів в моделюванні систем. Міжнародні документи в галузі інформаційної безпеки. Нормативні документи з питань безпеки комп'ютерних систем в США. Процесний та системний підхід до створення СУІБ. Створення комплексної СУІБ (процесний підхід). Стандарти управління інформаційною безпекою. Стандарти серії ДСТУ СУІБ. Системні рішення питань управління ІБ в організаціях різного рівня та форм власності. Методика формування нормативних (розпорядчих та методичних) документів в процесі впровадження та функціонування СУІБ. Документи в процесі впровадження та функціонування СУІБ. Розробка концепції, положення та функціональних обов'язків посадових осіб для експлуатації СУІБ. Документаційне забезпечення СУІБ. Реалізація цілей в управлінні активами в СУІБ
Тема 3. Розробка політики інформаційної безпеки та впровадження системи управління інформаційною безпекою. **Знати:** методики визначення напрямків, об'єктів та активів що підлягають захисту (інформаційні та технічні ресурси), порядок формування політики ІБ на підприємстві, структуру політики ІБ підприємства та процес її розробки, вимоги до побудови політики безпеки, програмні комплекси для створення і перевірки СУІБ, порядок супроводження процесу функціонування СУІБ. **Вміти:** розробляти політику інформаційної безпеки підприємства та використовувати програмні комплекси для створення і перевірки СУІБ. **Формування компетентностей:** КЗ1, КФ2, КФ4, КФ6. **Результати навчання:** РН9, РН11, РН14. **Рекомендовані джерела:** 1, 3, 5, 7, 9–13.			
Методика визначення напрямків, об'єктів та активів що підлягають захисту (інформаційні та технічні ресурси)	Лекція 7 2 год		Лекція-візуалізація
Структура політики інформаційної безпеки підприємства та процес її розробки: розробка документів політики інформаційної безпеки стратегічного рівня	Пз 13 2 год	3 бали	Практичні заняття проводяться на основі кейсів та практичних завдань із розробки документів політики інформаційної безпеки різних рівнів, а також з прикладами політик та нормативних документів забезпечення інформаційної безпеки.
Структура політики інформаційної безпеки підприємства та процес її розробки: розробка документів політики інформаційної безпеки тактичного рівня	Пз 14 2 год	3 бали	
Формування політики інформаційної безпеки на підприємстві	Лекція 8 2 год		Лекція-візуалізація
Структура політики інформаційної безпеки підприємства та процес її розробки: розробка документів політики інформаційної безпеки операційного рівня	Пз 15 2 год	3 бали	Практичні заняття проводяться на основі кейсів та практичних завдань із розробки документів політики

Програмні комплекси СУІБ. Можливості програмних продуктів SIEM у вирішенні задач інформаційної безпеки	Пз 16 2 год	3 бали	інформаційної безпеки із використанням програмних комплексів СУІБ. Застосовуються методи аналізу, моделювання з застосуванням спеціалізованих програмних продуктів для перевірки та забезпечення інформаційної безпеки.
Супроводження процесу функціонування системи управління інформаційною безпекою	Лекція 9 2 год		Лекція-візуалізація
Програмні комплекси для перевірки СУІБ	Пз 17 2 год	3 бали	Практичні заняття проводяться на основі кейсів та практичних завдань з демонстрацією можливостей SIEM і спеціалізованих програмних продуктів для перевірки та забезпечення інформаційної безпеки.
Тема 3. Розробка політики інформаційної безпеки та впровадження системи управління інформаційною безпекою	Самостійна робота 12 год	7 балів	**Питання для самостійного опрацювання:** Методика визначення напрямків, об'єктів та активів що підлягають захисту. Поняття інформаційних ресурсів. Специфіка інформаційних ресурсів організації, які підлягають захисту. Формування політики ІБ на підприємстві. Структура політики інформаційної безпеки на підприємстві та процес її розробки. Розробка документів політики ІБ вищого, середнього та нижчого рівнів. Підтримка політики інформаційної безпеки на підприємстві. Програмні засоби управління процесами забезпечення інформаційної безпеки. Програмні комплекси для створення і перевірки СУІБ на відповідність вимогам стандартам сімейства ISO. Програмна підтримка аналізу ризиків. Супроводження процесу функціонування СУІБ.
Іспит	Пз 18 2 год	30 балів	Письмова відповідь на контрольні питання білету.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет.
Віртуальне навчальне середовище на платформі GWE.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Якименко Ю. М., Савченко В. А., Легомінова С. В. Системний аналіз інформаційної безпеки: сучасні методи управління : підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf
2. Данілова Е. І. Концепція системного підходу до управління економічною безпекою підприємства : монографія. Вінниця : Європейська наукова платформа, 2020. 342с. URL: https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859
3. 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
4. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib
5. Kathryn Knerler, Ingrid Parker, Carson Zimmerman. 11 Strategies of a World-Class Cybersecurity Operations Center. 2022 The MITRE Corporation. 452 p.
6. Антонюк Б. П., Антонюк О. П. Технології інформаційного менеджменту: курс лекцій для студентів спеціальностей 014.09 Середня освіта (Інформатика) та 113 Прикладна математика Луцьк: Вежа-друк, 2022. 95 с.
7. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
8. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш.

справ, 2020. – 144 с.
9. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
10. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. С 50 Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.
11. Савченко В. А., Хавер А. В. Метод розрахунку кіберстійкості 2-1 рівнів моделі Purdue проти спеціалізованого технологічного троянського програмного забезпечення. Системи і технології зв'язку, інформатизації та кібербезпеки. 2025, № 7, 147-164. https://doi.org/10.58254/viti.7.2025.14.147
12. Олександр Лаптєв, Віталій Савченко, Алла Кобозева, Анатолій Салій, Тимур Куртсеітов. Методи оцінки захищеності інформації в мережах зв'язку. Кібербезпека: освіта, наука, техніка. 2025. Том 3 № 27. С. 522-533. https://doi.org/10.28925/2663-4023.2025.27.767
13. Савченко, В. А. (2024). Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації. Зв'язок, 3(169). 12-17. DOI: 10.31673/2412-9070.2024.031217
14. Савченко, В. А., & Рибальченко, О. Г. (2024). Побудова ефективної системи мережевої безпеки підприємства на основі методу аналізу ієрархій показників якості. Сучасний захист інформації, 1(57), 6–14. https://doi.org/10.31673/2409-7292.2024.010001
15. Савченко, В. А., Смолєв, Є. С., & Гамза, Д. Є. (2023). Методика виявлення аномалій взаємодії користувачів з інформаційними ресурсами організації. Сучасний захист інформації, 4(56), 6–12. https://doi.org/10.31673/2409-7292.2023.030101
16. Хавер, А. В.,& Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002
17. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev, V. Savchenko and others. – Kharkiv: PC Technology Center, 2023. – 168 p. https://doi.org/10.15587/978-617-7319-72-5

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 семінарських 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 здобувач 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 здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

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

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	51 бал
	• Самостійна робота	19 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит: письмова відповідь на контрольні питання.	30 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні категорії Б	5 балів

- Стаття у рецензованому виданні (Scopus, Web of Science)			10 балів
Сертифікат про підвищення кваліфікації за тематикою дисципліни			5 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти – **10 балів**.			
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Здобувач 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 Здобувач 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 здобувача 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 (A)
82-89	Здобувач 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 здобувачу 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	Здобувач 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	Здобувач 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	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень	Задовільно / Зараховано (D)

	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. .	дисципліни.	
60-66	Здобувач 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, здобувач 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	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача 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*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач 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**		