СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

Лектор курсу	**Якименко Юрій Михайлович**, кандидат військових наук, доцент, доцент кафедри "Управління інформаційною та кібернетичною безпекою"	**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**yakum14@ukr.net; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/category.php?id=216
Галузь знань	12 Інформаційні технології	**Рівень вищої освіти**	магістр
Спеціальність	125 Кібербезпека та захист інформації	**Семестр**	9
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
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у студентів базових теоретичних знань, умінь і практичних навичок, необхідних для використання системного підходу в застосовуванні сучасних способів, методів та засобів щодо створення систем управління інформаційною безпекою (СУІБ) .

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ-1. Здатність застосовувати знання у практичних ситуаціях. **КЗ-6.** Здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.	**КФ1.** Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. **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 ІБ інформаційної безпеки та/або кібербезпеки. **КФ4.** Здатність аналізувати, розробляти і супроводжувати систему управління ІБ інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики ІБ 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 ІБ

	інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання (РН)

РН6. Аналізувати та оцінювати захищеність систем,комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики ІБ інформаційної безпеки.
РН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН 14. 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.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН26. Здатність використовувати професійно профільовані знання й практичні навички для розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами.
РН29. Уміти застосовувати системний підхід для побудови системи управління (менеджменту) інформаційною безпекою організації (підприємства), яка визначає загальну організацію і класифікацію системи даних, систему доступу, напрямки планування, відповідальність співробітників, використання оцінки ризиків, тощо в контексті ІБ інформаційної безпеки.
РН30. Уміти застосовувати сучасні способи, методи та засоби управління наступними аспектами захисту: політикою безпеки, архітектурою захисту, механізмами захисту та засобами захисту.
РН31. На основі інформації, одержаної у ході дослідження об'єкта інформаційної діяльності замовника та результатів аналізу ризиків, розробляти рекомендації щодо удосконалення системи управління інформаційною безпекою, застосування яких дозволить мінімізувати ризики та формулювати перелік уразливостей.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1 «ЗАГАЛЬНІ ПОЛОЖЕННЯ ПО СТВОРЕННЮ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»			
Тема 1. ***Основні поняття та принципи створення системи управління інформаційною безпекою.*** ***<u>Знати</u>***: 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	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Лекція 3		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 1		Аналіз стану проблем управління інформаційною безпекою підприємства - на прикладах. Обговорення результатів

системного підходу в дослідженні СУІБ, методи досліджень СУІБ, системні рішення питань вимірювання ефективності СУІБ, методологію побудови ефективної СУІБ. ***<u>Вміти:</u>*** проводити дослідження та використовувати методологію організаційного забезпечення в вирішенні проблем управління ІБ і побудови ефективної СУІБ. ***<u>Формування компетенцій:</u>*** КЗ1, КФ1, КФ2 ***<u>Результати навчання:</u>*** РН6, РН8, РН9, РН11, РН14, РН30 ***<u>Рекомендовані джерела:</u>*** 1,3, 5, 9-13	Практичне заняття 2		Аналіз концептуальної схеми забезпечення ІБ. Обговорення результатів
	Практичне заняття 3		Аналіз методичних інструментів в дослідженнях СУІБ. Обговорення результатів
	Практичне заняття 4		Аналіз і синтез як методи в процесах управління СУІБ Обговорення результатів
	Практичне заняття 5		Вимірювання ефективності СУІБ - на прикладах. Обговорення результатів
	Практичне заняття 6		Методологічні підходи до дослідження СУІБ. Обговорення результатів
Тема 2. ***Концепції та моделі системи управління інформаційною безпекою.*** ***<u>Знати</u>***: 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. ***<u>Вміти</u>***: розробляти концепції, положення та функціональні обов’язки посадових осіб для експлуатації СУІБ; на основі аналізу результатів досліджень розробляти рекомендації щодо удосконалення СУІБ. ***<u>Формування компетенцій:</u>*** КЗ1, КФ4, КФ6 ***<u>Результати навчання:</u>*** РН8, РН9, РН11, РН14, РН23, РН29, РН30 ***<u>Рекомендовані джерела:</u>*** , 4-6, 10-14	Лекція 4	5,5*	Лекція-візуалізація
	Лекція 5		Лекція-візуалізація, експрес-опитування студентів
	Лекція 6		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 7		Реалізація процесного підходу до побудови СУІБ - на прикладі. Обговорення результатів
	Практичне заняття 8		Реалізація системного підходу до побудови СУІБ - на прикладі. Обговорення результатів
	Практичне заняття 9		Вивчення вимог стандартів серії ДСТУ ISO 27001- 27003 . Обговорення їх змісту
	Практичне заняття 10		Організація сертифікаційного аудиту та наглядових аудитів
	Практичне заняття 11		Розробка документів функціонування СУІБ. Обговорення результатів
	Практичне заняття 12		Модульний контроль №1. Виконання кваліфікаційних завдань. Тестування
Тема 1. Основні поняття та принципи створення системи управління інформаційною безпекою **Тема 2.** Концепції та моделі системи управління ІБ	Самостійна робота		1. Основні напрямки розвитку менеджменту в сфері ІБ 2. Проблеми управління ІБ 3. Комплексні проблеми в інформаційній сфері України і методи їх запобігання та ліквідації 4. Десять кроків до надійної системи ІБ

			5. Загальна методологія організаційного забезпечення ІБ 6. Особливості нормативно-правового забезпечення СУІБ 7. Методологія організаційного забезпечення ІБ на рівні великих постачальників інформаційних систем 8. Об'єктивні фактори, як передумови становлення інформаційного права України 9. Організаційне забезпечення ІБ на рівні окремих великих компаній. 10. Методи досліджень СУІБ 11. Дослідження як функція управління 12. Досвід створення СУІБ 13. Управління активами в СУІБ 14. Документаційне забезпечення СУІБ 15. Моделювання СУІБ 16. Принципи системного і процесного підходів в моделюванні систем 17. Міжнародні документи в галузі інформаційної безпеки. 18. Нормативні документи з питань безпеки комп'ютерних систем в США. 19. Процесний та системний підхід до створення СУІБ 20. Створення комплексної СУІБ (процесний підхід) 21. Стандарти управління інформаційною безпекою 22. Стандарти серії ДСТУ СУІБ 23. Системні рішення питань управління ІБ в організаціях різного рівня та форм власності 24. Методика формування нормативних (розпорядчих та методичних) документів в процесі впровадження та функціонування СУІБ 25. Документи в процесі впровадження та функціонування СУІБ 26. Розробка концепції, положення та функціональних обов’язків посадових осіб для експлуатації СУІБ 27. Документаційне забезпечення СУІБ 28. Реалізація цілей в управлінні активами в СУІБ
Розділ 2 «РЕАЛІЗАЦІЯ МЕТОДИЧНИХ ПІДХОДІВ ДО ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»			
Тема 3. ***Розробка політики інформаційної безпеки та впровадження системи управління інформаційною безпекою.*** ***<u>Знати</u>***: методики визначення напрямків, об’єктів та активів що	Лекція 7	5,5*	Лекція-візуалізація
	Лекція 8		Лекція-візуалізація, експрес-опитування студентів

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 компетенцій:*** КЗ6, КФ4, КФ6 ***Результати навчання:*** РН6 РН11, РН26, РН29, РН31 ***Рекомендовані джерела:*** 9-14	Лекція 9		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 13		Структура політики інформаційної безпеки підприємства та процес її розробки: розробка політики ІБ(вищого). Обговорення результатів
	Практичне заняття 14		Структура політики інформаційної безпеки підприємства та процес її розробки: розробка документів політики ІБ середнього рівня. Обговорення результатів
	Практичне заняття 15		Структура політики інформаційної безпеки на підприємстві та процес її розробки: розробка документів політики ІБ нижчого рівня. Обговорення результатів
	Практичне заняття 16		Програмні комплекси для створення СУІБ. Можливості програмних продуктів SIEM у вирішенні задачі управління ІБ
	Практичне заняття 17		Програмні комплекси для перевірки СУІБ
	Практичне заняття 18		Модульний контроль №2. Виконання кваліфікаційних завдань. Тестування
Тема 3. Розробка політики та впровадження системи управління ІБ	Самостійна робота		1. Методика визначення напрямків, об’єктів та активів що підлягають захисту 2. Поняття інформаційних ресурсів 3. Специфіка інформаційних ресурсів організації, які підлягають захисту 4. Формування політики ІБ на підприємстві 5. Структура політики інформаційної безпеки на підприємстві та процес її розробки 6. Розробка документів політики ІБ вищого, середнього та нижчого рівнів 7. Підтримка політики інформаційної безпеки на підприємстві 8. Програмні засоби управління процесами забезпечення інформаційної безпеки 9. Програмні комплекси для створення і перевірки СУІБ на відповідність вимогам стандартам сімейства ISO 10. Програмна підтримка аналізу ризиків 11. Супроводження процесу функціонування СУІБ

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

1. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В. Л. Бурячок та ін. Київ, 2015. 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd
2. Роїк О. М., Шиян А. А., Нікіфорова Л. О. Системний аналіз: навчальний посібник. Вінниця, 2015. 83 с. URL: http://nikiforova.vk.vntu.edu.ua/file/bfb63146b18f718fe1ff1ed4ce9b9a58.pdf
3. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою. Професійний розвиток фахівців у системі освіти дорослих: історія, теорія, технології : програма IV-ої Всеукраїнської Інтернет-конференції / за наук. ред. В.В. Сидоренко; упорядкування Я. Л. Швень, М. І. Скрипник. Київ: Агроосвіта, 16 жовтня 2019 р. 41-43 с.
4. Якименко Ю. М. Про підхід до створення системи інформаційної безпеки в організації. Інформаційна безпека України : зб. наук. доп. та тез НТК. Київ : Київський національний університет імені Тараса Шевченка, 23-24 березня 2017 р. 372-376 с.
5. Маркіна І.А. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. Харків : ХНАДУ, 2016. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf
6. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко та ін. Київ : Університет «Україна», 2013. 203 с. URL: http://er.nau.edu.ua/handle/NAU/20105 , http://er.nau.edu.ua:8080/handle/NAU/20105
7. 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
8. 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
9. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib
10. 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
11. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / О. Г. Корченко та ін. Київ : Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. 190с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
12. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
13. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014), Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
14. ДСТУ ISO/IEC 27003:2018 (ISO/IEC 27003:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова . (ISO/IEC 27003:2010).
15. ДСТУ ISO/IEC 27009:2018 (ISO/IEC 27009:2016, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги.
16. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT) Настанови щодо проведення аудитів систем управління.

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
РУБІЖНЕ ОЦІНЮВАННЯ (КОНТРОЛЬ)	Контроль № 1 «ЗАГАЛЬНІ ПОЛОЖЕННЯ ПО СТВОРЕННЮ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка – 15балів
	Контроль № 2 « ОСНОВНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	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 іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні	Відмінно / Зараховано (А)

	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.	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.	
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)
5 - 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 екзамену.	**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*