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

СИЛАБУС НАВЧАЛЬНОЇ КОМПОНЕНТИ
«Управління безпекою інформаційних мереж»

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 GWE –** https://classroom.google.com/c/ODQ1NjMxNTAxOTIz?cjc=ms7tz2jp	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	2	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Вибіркова 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

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Дисципліни професійної підготовки.
Освітні компоненти для яких є базовою	Кваліфікаційна робота.

Мета курсу:	Формування у здобувачів освіти знань і навичок щодо застосування сучасних методів, засобів і технологій захисту інформаційних мереж, а також оволодіння принципами та інструментами автоматизації процесів управління кібербезпекою з метою забезпечення надійного функціонування мережевих систем в умовах сучасних загроз.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.	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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо запобігання та аналізу кіберінцидентів в цілому.

Програмні результати навчання (ПРН)			
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. 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 фізико-математичних 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. 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.			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема,опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Інформаційна мережа, базові поняття та проблеми функціонування **Знати:** базові поняття та принципи функціонування інформаційних мереж, основи управління їх безпекою, типові ризики, загрози й вразливості, міжнародні стандарти серії ISO/IEC 27000 та методологію управління IT від COBIT, принципи політики безпеки й концепцію поглибленого захисту (Defense-in-Depth), а також сучасні технології виявлення загроз і атак на інформаційні мережі. **Вміти:** ідентифікувати та класифікувати ризики, загрози й вразливості в інформаційних мережах, застосовувати положення міжнародних стандартів та політик безпеки, аналізувати загрози для локальних корпоративних мереж, використовувати методи та засоби забезпечення мережевої безпеки, а також практично застосовувати технології виявлення загроз і атак для підвищення захищеності мережевої інфраструктури. **Формування компетентностей:** КЗ1, КЗ2, КФ1, КФ6. **Результати навчання:** РН2, РН3, РН5. **Рекомендовані джерела:** 1–6, 10–13.			
Основи управління безпекою інформаційних мереж	Лекція 1 2 год		Лекція-візуалізація
Основи управління інформаційними мережами	Пз 1 2 год	2 бали	Практичні заняття проводяться у формі роботи з реалістичними кейсами та проблемними ситуаціями, з використанням аналізу та класифікації ризиків, групових обговорень, дискусій і завдань на систематизацію понять «ризик», «загроза», «вразливість» у контексті управління інформаційними мережами.
Ризик, загроза, вразливість. Систематизація операційних ризиків, пов'язаних з інформаційною безпекою мереж	Пз 2 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити основні цілі управління безпекою інформаційних мереж і зв'язок із принципами CIA, ознайомитися з елементами методології COBIT та їх роллю в СУІБ, розглянути методи оцінки ризиків і загроз у корпоративних мережах, проаналізувати стандарти серії ISO/IEC 27000 та їх застосування, а також вивчити приклади політик безпеки для контролю доступу, моніторингу подій і запобігання інцидентам.
Аналіз загроз безпеці інформаційних мереж	Лекція 2 2 год		Лекція-візуалізація

Міжнародні стандарти серії ISO 27000. СУІБ	Пз 3 2 год	2 бали	Практичні заняття проводяться у формі вивчення нормативних документів і стандартів ISO/IEC 27000, розбору кейсів щодо побудови та функціонування СУІБ, а також дослідження прикладів загроз для локальних корпоративних мереж із використанням методів групового обговорення, дискусій та практичних завдань на ідентифікацію й оцінювання загроз.
Аналіз загроз безпеці локальних корпоративних мереж	Пз 4 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити класифікацію та характеристики загроз інформаційним мережам, ознайомитися з методами їх виявлення й оцінювання, розглянути приклади реальних кібератак і їх наслідків, а також дослідити підходи до побудови систем протидії та мінімізації ризиків.
Забезпечення інформаційної безпеки мереж	Лекція 3 2 год		Лекція-візуалізація
Методологія управління IT від COBIT	Пз 5 2 год	2 бали	Практичні заняття проводяться у формі вивчення методології управління IT від COBIT та політик безпеки інформаційних мереж, розбору кейсів щодо впровадження процесів управління та розробки політик безпеки, а також виконання практичних завдань із моделювання процесів і оцінки ефективності політик із використанням методів групового обговорення, дискусій та практичних вправ.
Політика безпеки інформаційної мережі	Пз 6 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити основні види загроз інформаційним мережам і їх характеристики, ознайомитися з методами ідентифікації та оцінки загроз, розглянути інструменти моніторингу та аналізу подій безпеки, проаналізувати типові кейси кібератак і їх наслідки, а також вивчити підходи до побудови заходів протидії загрозам і зменшення ризиків.
Концепція поглибленого захисту мережі (Defense-in-Depth)	Лекція 4 2 год		Лекція-візуалізація
Технології виявлення загроз інформаційним мережам	Пз 7 2 год	2 бали	Практичні заняття проводяться у формі вивчення сучасних технологій виявлення загроз і атак на інформаційні мережі, розбору кейсів щодо ідентифікації та реагування на інциденти безпеки, а також виконання практичних завдань із використанням інструментів моніторингу та аналізу подій із застосуванням методів групового обговорення, дискусій та практичних вправ.
Технології виявлення атак на інформаційні мережі	Пз 8 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити основи концепції поглибленого захисту мережі (Defense-in-Depth), ознайомитися з багаторівневими шарами захисту та їх функціями, розглянути взаємодію технічних, організаційних та процедурних заходів, проаналізувати приклади реалізації Defense-in-Depth у корпоративних мережах, а також оцінити ефективність комбінованих заходів для зменшення ризиків і запобігання інцидентам.
Тема 2. Технології управління безпекою інформаційних мереж.			

Знати: сучасні технології та методи управління безпекою інформаційних мереж, включаючи ідентифікацію та автентифікацію користувачів, електронний цифровий підпис, хешування та біометричні методи; принципи захисту корпоративних мереж, кінцевих точок (EDR, UBA, UEBA, DLP), технології введення в оману (Deception Technology); особливості застосування засобів захисту на різних рівнях моделі OSI; підходи до аналізу захищеності мереж, безпеки мобільних і хмарних технологій; призначення та можливості систем SIEM, а також роль управління персоналом і фізичної безпеки у комплексному захисті мереж. **Вміти:** застосовувати сучасні технології автентифікації та захисту інформаційних мереж, аналізувати їх захищеність і виявляти вразливості, використовувати методи протидії загрозам кінцевих точок і корпоративних мереж, впроваджувати багаторівневий захист відповідно до моделі OSI, оцінювати ризики для мобільних пристроїв і хмарних сервісів, працювати з системами SIEM для моніторингу та реагування на інциденти, а також організовувати заходи з управління персоналом і фізичною безпекою для підвищення стійкості мережевої інфраструктури. **Формування компетентностей:** КЗ2, КЗ4, КФ6, КФ7. **Результати навчання:** РН5, РН8, РН11. **Рекомендовані джерела:** 1–4, 7–9, 14–15.			
Технології ідентифікації та автентифікації користувачів мережі	Лекція 5 2 год		Лекція-візуалізація
Електронний цифровий підпис і функція хешування	Пз 9 2 год	2 бали	Практичні заняття проводяться у формі вивчення технологій електронного цифрового підпису, функцій хешування та біометричних методів у забезпеченні безпеки інформаційних мереж, а також виконання практичних завдань із використанням відповідних програмних комплексів.
Біометричні методи в управлінні безпекою інформаційних мереж	Пз 10 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити основні технології ідентифікації та автентифікації користувачів мережі, ознайомитися з методами паролів, багатофакторної та біометричної автентифікації, розглянути протоколи та стандарти забезпечення безпечного доступу, проаналізувати кейси впровадження автентифікації в корпоративних мережах, а також оцінити ефективність різних методів захисту від несанкціонованого доступу.
Технології та засоби захисту корпоративних мереж	Лекція 6 2 год		Лекція-візуалізація
Технології запобігання й протидії загрозам кінцевих точок (EDR, UBA, UEBA, DLP).	Пз 11 2 год	2 бали	Практичні заняття проводяться у формі вивчення технологій запобігання та протидії загрозам кінцевих точок (EDR, UBA, UEBA, DLP) та використання технологій введення в оману (Deception Technology) для захисту інформаційно-телекомунікаційних систем, а також виконання практичних завдань із застосуванням відповідних програмних комплексів.
Використання технологій введення в оману в захисті ІТС (Deception Technology).	Пз 12 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити основні технології та засоби захисту корпоративних мереж, ознайомитися з міжмережевими екранами, системами виявлення та запобігання вторгнень, засобами шифрування та контролю доступу, розглянути кейси впровадження комплексного захисту, а також оцінити ефективність різних підходів для забезпечення конфіденційності, цілісності та доступності інформації.
Модель OSI	Лекція 7 2 год		Лекція-візуалізація

Технології захисту на канальному, транспортному й мережевому рівнях	Пз 13 2 год	2 бали	Практичні заняття проводяться у формі вивчення технологій захисту інформаційних мереж на канальному, транспортному та мережевому рівнях, а також на прикладному, представницькому й сеансовому рівнях, розбору кейсів щодо їх впровадження та ефективності, а також виконання практичних завдань із використанням відповідних програмних комплексів.
Технології захисту на прикладному, представницькому й сеансовому рівнях	Пз 14 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити сім рівнів моделі OSI та їх функції, ознайомитися з прикладами протоколів на кожному рівні, розглянути процес взаємодії між рівнями під час передачі даних, а також дослідити роль моделі OSI у забезпеченні сумісності та безпеки мережевих систем.
Технологія аналізу захищеності інформаційних мереж	Лекція 8 2 год		Лекція-візуалізація
Безпека мобільних пристроїв у корпоративних мережах	Пз 15 2 год	2 бали	Практичні заняття проводяться у формі вивчення технологій забезпечення безпеки мобільних пристроїв у корпоративних мережах та захисту хмарних технологій, розбору кейсів щодо їх впровадження та ефективності, а також виконання практичних завдань із використанням відповідних програмних комплексів.
Безпека хмарних технологій	Пз 16 2 год	2 бали	
Самостійна робота	Самостійна робота 11 год	3 бали	Вивчити модель OSI, ознайомитися з її сімома рівнями та їх функціями, розглянути взаємодію протоколів і сервісів на різних рівнях, проаналізувати приклади передачі даних у мережі відповідно до OSI, а також оцінити роль кожного рівня у забезпеченні безпеки та надійності інформаційних мереж.
Системи управління інформацією та подіями безпеки (SIEM)	Лекція 9 2 год		Лекція-візуалізація
Управління персоналом і фізичною безпекою інформаційних мереж	Пз 17 2 год	2 бали	Практичне заняття проводиться у формі дослідження методів управління персоналом та забезпечення фізичної безпеки інформаційних мереж на основі розбору кейсів щодо організації доступу, контролю дій співробітників і захисту критичних об’єктів з виконанням практичних завдань.
Самостійна робота	Самостійна робота 8 год	2 бали	Вивчити принципи роботи систем SIEM, ознайомитися з методами збору та аналізу подій безпеки, розглянути кейси виявлення інцидентів, а також оцінити ефективність SIEM для моніторингу та захисту інформаційних мереж.
Залік	Пз 18 2 год	40 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. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПІ. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
3. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навч. посіб. Київ : ДУТ, 2023. 125 с. https://duikt.edu.ua/uploads/p_287_73266008.pdf
4. Рабчун Д.І. Аналіз та оцінка уразливостей інформаційних систем. Навчальний посібник. Київ: ДУТ, 2021, 86 с https://duikt.edu.ua/uploads/p_287_73266008.pdf
5. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с. URL: https://ela.kpi.ua/bitstream/123456789/38326/1/Information_security_NP.pdf
6. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А. Інформаційна безпека в комп'ютерних мережах : навч. посіб. /; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницький : Лисенко В.Ф., 2020. 295 с. URL:http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf
7. 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. https://duikt.edu.ua/uploads/l_1487_78606346.pdf
8. 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
9. 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
10. Савченко, В., Поночовний, П. і Аверічев, І. 2024. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. Прикладні проблеми комп'ютерних наук, безпеки та математики. 3 (Вер 2024), 71–81. https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127/97
11. 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
12. Савченко В.А. Прогнозування динаміки підозрілої активності у мережі на основі аналізу мережевого трафіку / Кожухівський А.Д., Ільїн О.Ю., Савченко В.А. Зв'язок. 2021. № 6(154). – С. 38– 47. https://doi.org/10.31673/2412-9070.2021.062630
13. Model of Connectivity in a Mobile MESH Network for a Group of Unmanned Aerial Vehicles. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 142-147 https://ieeexplore.ieee.org/document/10024235
14. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network / Oleksandr Laptiev, Nataliia Lukova-Chuiko, Serhii Laptiev, Vitaliy Savchenko, Tetiana Laptieva and Serhii Yevseiev. Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології». 13-19 вересня 2021 року. Forum "Digital Reality", September 13 − 19, 2021, Odesa, Ukraine. P.8–16. https://ceur-ws.org/Vol-3200/paper1.pdf
15. Development of Routing Algorithm for Self-Organizing Radio Networks / Breslavskyi, V., Laptiev, O., Savchenko, V., Shuklin, G. & Biehun, A. International Journal of Science and Engineering Investigations (IJSEI), (2020). vol. 9(107), 46-50. http://www.ijsei.com/papers/ijsei-910720-08.pdf

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	34 бали
	• Самостійна робота	26 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ *Залік*	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік: письмова відповідь на контрольні питання.	40 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 100 балів

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис в заліковій 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 (А)
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 (В)
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	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми	Добре / Зараховано (С)

	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.	дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
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 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	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*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.