

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КІБЕРБЕЗПЕКА БАНКІВСЬКИХ ТА КОМЕРЦІЙНИХ СТРУКТУР»

Лектор курсу			Ахрамович Володимир Миколайович, кандидат технічних наук, доцент, кафедри систем інформаційного та кібернетичного захисту		Контактна інформація лектора (e-mail), сторінка курсу в Moodle		e-mail: ptbd_dut@ukr.net ; сторінка курсу в Moodle – http://dl.dut.edu.ua/course/view.php?id=1195	
Галузь знань					Рівень вищої освіти		бакалавр	
Спеціальність					Семестр		5	
Освітня програма					Тип дисципліни		Вибіркова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
	5	150	Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
			18	-	18	18	96	

АНОТАЦІЯ КУРСУ

Мета курсу:	<p>формування у студентів необхідної системи знань з основ кібербезпеки банківських та комерційних структур, діяльності з захисту інформації її регулювання, опанування студентами необхідних теоретичних знань із вжиття організаційних заходів для забезпечення інформаційної безпеки в банківських та комерційних системах, створення комплексу технічного захисту інформації на об'єктах інформаційної діяльності. Вивчення методів та форм організаційного забезпечення технічного захисту інформації. Освоєння сучасних засобів технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>надання практичних навиків по розробці організаційних та технічних документальних матеріалів зі створення комплексу технічного захисту інформації, оформленню експлуатаційної документації та застосуванню сучасних засобів технічного захисту інформації.</p>
--------------------	---

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	Фахові компетентності (ПП)
<p>ЗК 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК 2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК 5. Здатність до пошуку, оброблення та аналізу інформації..</p>	<p>ПП 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.</p> <p>ПП 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки.</p> <p>ПП 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах..</p>

Програмні результати навчання (ПРН)

<p>ПРН 2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність</p> <p>ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.</p>

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 7. Діяти на основі законодавчої та нормативноправової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та кібербезпеки.

ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативноправових документів.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 18. Використовувати програмні та програмноапаратні комплекси захисту інформаційних ресурсів.

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційнотелекомунікаційних системах.

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1 «Організація робіт з інформаційного та кібернетичного захисту інформації в банківських та комерційних системах»			
<p>Тема 1. <i>Загальна ситуація з умовами кібербезпеки банків та комерційних підприємств.</i></p> <p>Знати: Загальну ситуацію з умовами безпеки банків та комерційних підприємств, комплексну безпеку банків та комерційних підприємств, функції керівника підрозділу безпеки банку, внутрішні та зовнішні загрози банку, обладнання і технічну укріпленість банків, організацію охорони установ банків, режими охорони, проблеми створення автоматизованих систем обробки даних (АСОД), проблеми застосування захисту. методологію захисту автоматизованих систем обробки інформації (АСОІ), загроза безпеці АСОІ.</p> <p>Вміти: . використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності, аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення, забезпечувати функціонування спеціального програмного забезпечення, щодо</p>	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Лекція 3		Лекція-візуалізація, експрес-опитування студентів

<p>захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. Формування компетенцій:ЗК1, ЗК2, ПП1,ПП2 Результати навчання:ПРН3, ПРН4, ПРН20 Рекомендовані джерела: 1, 4–10</p>			
<p>Тема 2. Інформаційна та кібербезпека в банківських та комерційних системах. Знати: мету, завдання, моделі та механізм промислового шпигунства, інформаційну безпеку суб'єкта підприємництва в Україні та світі, методи захисту в банківській діяльності, СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ, Вимоги (ISO/IEC 27001:2005, MOD, методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України, положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, інформація з обмеженим доступом у банківській діяльності, система захисту інформації в банку, вимоги до захисту інформації при здійсненні переказів грошових коштів в Платіжній Системі Вестерн Юніон, шифрування даних за допомогою архіваторів та пошук паролів, пошук паролів у документах Microsoft Office за допомогою спеціальних програм, шифрування даних за допомогою спеціальних програм та утиліт, тестування дисків та відновлення даних на дисках, які попередньо видалені , або видалені при форматуванні, захист інформації при застосуванні особистої системи мережевого захисту Comodo Firewall, налагодження захисту даних комп'ютерної мережі при використанні ОС Windows XP, Windows 10 та Microsoft Office, антивірусні програми, видалення програм з комп'ютера за допомогою різного програмного забезпечення.</p>	<p>Лекція 4</p> <p>Практичне заняття 1</p> <p>Лекція 4</p> <p>Практичне заняття 1</p> <p>Практичне заняття 2</p>	<p>5,5*</p>	<p>Лекція-візуалізація, експрес-опитування студентів</p> <p>Усне опитування, навчальна дискусія, обговорення ситуаційного завдання</p> <p>Лекція-візуалізація, експрес-опитування студентів</p> <p>Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни</p> <p>Тестування, навчальна дискусія, кейс-метод</p>
<p>Вміти: організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем професійній діяльності, оцінювати їхню ефективність, використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності, аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p>	<p>Лекція 5</p> <p>Практичне заняття 3</p> <p>Лекція 6</p> <p>Практичне заняття 4</p> <p>Лабораторне заняття 1</p> <p>Лекція 7</p> <p>Практичне заняття 5</p> <p>Лабораторне заняття 2</p> <p>Лабораторне заняття 3</p>	<p>5,5*</p>	<p>Лекція-візуалізація, експрес-опитування студентів</p> <p>Мозковий шторм, навчальна дискусія, вирішення практичних задач</p> <p>Лекція-візуалізація, експрес-опитування студентів</p> <p>Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни</p> <p>Комп'ютерний клас. Шифрування даних за допомогою архіваторів та пошук паролів</p> <p>Лекція-візуалізація, експрес-опитування студентів</p> <p>Тестування, навчальна дискусія, вирішення практичних задач</p> <p>Комп'ютерний клас. Пошук паролів у документах Microsoft Office за допомогою спеціальних програм</p> <p>Комп'ютерний клас. Шифрування даних за допомогою спеціальних програм та утиліт</p>

<p>реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів, забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент, використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів, застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах, забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС, вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та кібербезпеки.</p> <p>Формування компетенцій:ЗК1, ЗК2, ЗК4, ЗК5,ПП1,ПП2,ПП3.</p> <p>Результати навчання:ПРН2, ПРН3, ПРН4 ПРН16 – ПРН20, ПРН22, ПРН23.</p> <p>Рекомендовані джерела: 1, 19.</p>	Лабораторне заняття 4		
	Лабораторне заняття 5		Комп'ютерний клас. Видалення даних за допомогою програми Disk Wiper
	Лабораторне заняття 6		Комп'ютерний клас. Тестування дисків та відновлення даних на дисках, які попередньо видалені, або видалені при форматуванні.
	Лабораторне заняття 7		Комп'ютерний клас. Захист інформації при застосуванні особистої системи мережевого захисту Comodo Firewall
	Лабораторне заняття 8		Комп'ютерний клас. Налаштування захисту даних комп'ютерної мережі при використанні ОС Windows XP, Windows 10 та Microsoft Office
	Лабораторне заняття 9		Комп'ютерний клас. Антивірусні програми
	Лабораторне заняття 9		Комп'ютерний клас. Видалення програм з комп'ютера за допомогою різного програмного забезпечення
	Лекція 8		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 6		Проведення модульного контролю
	Самостійна робота		<ol style="list-style-type: none"> 1. Категорії інформаційної безпеки з точки зору інформації та інформаційних систем. 2. Категоризація інформації 3. Технічні, програмно-апаратні та адміністративні засоби захисту інформації. 4. Комплексна безпека банків та комерційних підприємств 5. Постанова НБУ про затвердження Правил з технічного захисту інформації 6. Рекомендації щодо побудови структурованих і локальних мереж. 7. Парольний захист інформації. 8. Визначення вимог з інформаційної безпеки банку 9. Аналіз ризиків 10. Ідентифікація загроз та вразливостей 11. Шифрування даних 12. Підготовка Положення щодо застосовності безпеки (перепусток) тощо. 13. Методологія захисту автоматизованих систем обробки інформації (АСОІ) 14. Загроза безпеці АСОІ.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проєктор;
- Комп'ютерний клас для проведення лабораторних та практичних занять.
 - Програмне забезпечення. Windows XP, 8,10, Microsoft Office, WinRar, WinZip, Ultra Zip Password Cracker 1.00 та Advanced ZIP Password Recovery 2.2, Advanced Rar Password Recovery 3, Advanced Office 97 Password Recovery. Super File Encryption ,T-CEC Pro. BestCrypt, Disk Wiper, Easy Recovery Professional, Victoria, McAfee Personal Firewall Plus, Comodo Firewall ,Revo Uninstaller. Iobit Uninstaller, NOD 32.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2019.-276с.
2. Головань СМ., Васюков І.В., Давиденко А.М., Хорошко В.О., Щербак Л.М. Основи організації електронного документообігу: У 2 т./ – К.: ДУІКТ, 2018. – Т. 1. – 230 с., Т. 2. – 233 с.
3. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М. Конфіденційне діловодство. Практикум: Навч. Посіб. – Луганськ: СНУ ім. В.Даля, 2020. – 180 с.
4. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2016. – 102 с.
5. Конахович Г.Ф. и др. Защита информации в телекоммуникационных системах.-К. «МК-Пресс», 2015. - 288 с.
6. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2015. – 432 с.
7. Бузов О.О. Защита информации от утечки по техническим каналам. Учебное пособие. М.: Гостехкомисия России, 2015. - 435 с.
8. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2016. – 108 с.
9. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник.-К. ДУІКТ, 2020. - 316 с.
10. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методи и средства защиты информации. – К: Арий, 2018, т. 1, 2 - 806 с.
11. Литвиненко В.К. Охрана, сопровождение грузов, денежных средств и ценных бумаг. М.: Арсин, 2019. 76с.
12. Лужецький В.А. Захист персональних даних. Навчальний посібник./ Лужецький В.А., Войтович О.П., Дудат'єв А.В – Вінниця: ВНТУ, 2019. – 487 с.
13. Лужецький В.А., Войтович О.П., Дудат'єв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-СУМ-Вінниця, 2019. – 240 с.
14. Мамаєв М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник – СПб.: Питер, 2017.
15. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2015. – 208с.
16. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2017.
17. Хорєв А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ "Аналитика", 2018. – 436 с.
18. Хорошко В.О., Чередниченко В.С., Шелест М.С. Основи інформаційної безпеки : К.: ДУІКТ, 2018. – 186 с.
19. Юдін О. К.Юдін О. К.Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ “НВП”ІНТЕРСЕРВІС”, 2019. – 716 с.

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.

<ul style="list-style-type: none"> 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 КONTРOЛЬ	<i>Робота на заняттях, у т.ч.:</i>	
	• 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
РУБЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КONTРOЛЬ)	Модульний контроль № 1 «ТЕОРЕТИЧНІ ОСНОВИ БІРЖОВОЇ ДІЯЛЬНОСТІ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «БІРЖОВА ТОРГІВЛЯ ТА ЇЇ ОСОБЛИВОСТІ»	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 <i>Іспит</i>	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 /затис в екзаменаційній відомості
001-06	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному	Відмінно / Зараховано (А)

	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.	поглибленому вивченні 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 вивченні 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 розглядалися 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)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутня.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не поставляється
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	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не

		окреслює мета та завдання дисципліни	<i>поставляється</i>
--	--	--------------------------------------	----------------------