СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОБМЕЖЕНОГО ДОСТУПУ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Ахрамович Володимир Миколайович, доктор технічних наук, професор, кафедри систем інформаційного та кібернетичного захисту</td><td>Контактна інформаціялектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail:ptbd_dut@ukr.net;
сторінка курсу в Moodle –
http://dl.dut.edu.ua/course/view.php?id=1195</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2"></td><td>Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2"></td><td>Семестр</td><td colspan="2">9</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2"></td><td>Тип дисципліни</td><td colspan="2">Вибіркова</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>6</td><td>180</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
18</td><td>Самостійна підготовка
126</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">формування у студентів необхідної системи знань з основ розкриття концептуальних засад із вжиття організаційних заходів для забезпечення інформаційної безпеки, створення комплексу технічного захисту інформації на об’єктах інформаційної діяльності з обмеженим доступом. Вивчення методів та форм організаційного забезпечення технічного захисту інформації. Освоєння сучасних засобів технічного захисту інформації на об’єктах інформаційної діяльності з обмеженим доступом.
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.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Фахові компетентності (ПП)</td></tr>
<tr><td colspan="4">ЗК 1. Здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним та самокритичним
ЗК 2. Вміння використовувати інформаційні і комунікаційні технології для впровадження технологій в інформаційній та безпекових сферах
ЗК 8. Вміння розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації</td><td colspan="5">ПП 1. Здатність до виявлення та формування актуальних наукових проблем, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх у усній акбо письмових формах перед фаховою і нефоховою аудиторією.
ПП 2. Здатність до обгрунтування та реалізації системи захисту інформаційних ресурсів з обмеженим доступом на об’єктах інформаційної діяльності.
ПП-5. Здатність до накопичення наукових та педагогічних вмінь та навичок , здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки.
ПП-8. Здатність до планування і реалізпції заходів із захисту інформації в ІКС; створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень.</td></tr>
</table>

	ПП-9 Здатність до проектування перспективнихсистем захисту інформації, застосовуючі сучасні методи і засоби їх аналізу та побудови. ПП-10. Здатність до підтримання комплексних систем інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації.

Програмні результати навчання (ПРН)

ПРН 7. Уміти обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об’єктах інформаційної діяльності.
ПРН 9. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності.
ПРН 10. Уміти здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.
ПРН 12. Володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності.
ПРН 13. Уміти застосовувати типові підходи до проектування захищених обєктів інформаційної діяльності.
ПРН 16. Уміти розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності.
ПРН 18. Здійснювати розроблення методик аналізу , синтезу, оптимізації та прогнозування якості процесів захисту інформації з обмеженим доступом на оюєктах інформаційної діяльності.
ПРН 26. Уміти застосовувати сучасні способи, методи та засоби захисту автоматизованих систем6 політику безпеки, архітектуру захисту, механізми та засоби захисту.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1 «Правове забезпечення та системи захисту інформації обмеженого доступу» »			
Тема 1. ***Правове забезпечення захисту інформації обмеженого доступу*** ***Знати***: історію (онтологію) розвитку технологій об’єктивного вираження спілкування між людьми, взаємозв'язок інформатики та права в інформаційному суспільств, системи правового регулювання соціальних інформаційних відносин, інформаційно-пошукові системи, закон України про захист інформації в інформаційно-телекомунікаційних системах, перелік відомостей, що становлять службову інформацію і яким присвоюється гриф з обмеженим доступом «для службового користування», кількісну оцінку стійкості парольного захисту, використання цифрового підпису і шифрування електронних повідомлень, злочини проти конфіденційності, цілісності і доступності комп'ютерних даних та	Лекція 1	5,5*	Лекція-візуалізація
	Практичне заняття 1		Усне опитування, навчальна дискусія,обговорення ситуаційного завдання
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 2		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Лабораторне заняття 1		Комп’ютерна аудиторія. 2 Кількісна оцінка стійкості парольного захисту

систем, злочини, пов'язані з використанням комп'ютерів, злочини, пов'язані з порушенням авторських і суміжних прав з використанням комп'ютерних даних і систем, злочин, пов'язані зі змістом даних. ***Вміти:*** Уміти обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів. ***Формування компетенцій:***ЗК1, ЗК2, ПП1 ***Результати навчання:***ПРН7, ПРН10 ***Рекомендовані джерела:*** 1, 3–10,14-20	Лабораторне заняття 2		Комп'ютерна аудиторія. Використання цифрового підпису і шифрування електронних повідомлень
	Лекція 3		Лекція-візуалізація, експрес-опитування студентів
Тема 2. ***Системи захисту інформації обмеженого доступу*** ***Знати***:комплексну систему захисту, об'єкти захисту та їхні властивості, розроблення й оцінювання захищених систем, загрози безпеці інформації, класифікацію атак, методику класифікації загроз STRIDE, наслідки дій порушників, положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації, типове положення про службу захисту інформації в автоматизованій системі, сканування мереж, захист від копіювання. прив'язку до апаратного забезпечення. використання реєстру, ***Вміти***: уміти обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності,, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. ***Формування компетенцій:***ЗК1, ЗК2, ПП1,ПП2,ПП8,ПП10 ***Результати навчання:***ПРН7, ПРН9, ПРН12, ПРН16 ***Рекомендовані джерела:*** 2–10,14-20	Лекція 4	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3		Усне опитування, навчальна дискусія,обговорення ситуаційного завдання
	Лабораторне заняття 3		Комп'ютерна аудиторія. Сканування мереж.
	Лабораторне заняття4		Комп'ютерна аудиторія. Захист від копіювання. Прив'язка до апаратного забезпечення. Використання реєстру
	Практичне заняття 4		Проведення модульного контролю
Розділ 2 «Уразливості та моделі захисту інформації обмеженого доступу»			

Тема 3. ***Аналіз уразливості систем захисту інформації з обмеженим доступом*** ***Знати***: захист програмного забезпечення від реасемблерів та налагоджувачів, системний підхід до захисту ПЗ, безпеку інформаційних ресурсів у ІКСМ, формування вимог до КСЗІ, захист інформації при застосуванні особистої системи мережевого захисту, технічне завдання на комплексну систему захисту інформації типового робочого місця зовнішнього користувача. ***Вміти***: обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, застосовувати типові підходи до проектування захищених обєктів інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. ***Формування компетенцій:***ЗК1, ЗК2, ЗК8,ПП1, ПП2,ПП8-ПП10 ***Результати навчання:***ПРН7, ПРН9 -ПРН13, ПП18, ПП26. ***Рекомендовані джерела:*** 1–21	Лекція 5	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Мозковий шторм, навчальна дискусія,обговорення ситуаційного завдання
	Лабораторне заняття 5		Комп'ютерна аудиторія. Захист інформації при застосуванні особистої системи мережевого захисту Comodo Firewall
	Практичне заняття 6		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
Тема 4. ***Моделі систем захисту інформації з обмеженим доступом*** ***Знати***: правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, методику оцінки захищеності інформації, ***Вміти:*** володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, застосовувати типові підходи до проектування захищених обєктів інформаційної діяльності,розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності, здійснювати розроблення методик аналізу , синтезу, оптимізації та прогнозування якості процесів захисту інформації з обмеженим доступом на оюєктах інформаційної діяльності, застосовувати сучасні способи, методи та засоби захисту автоматизованих систем6 політику безпеки, архітектуру захисту, механізми та засоби захисту. ***Формування компетенцій:***ЗК1, ЗК2, СК1 ***Результати навчання:***ПРН7, ПРН12, ПП8-ПП10, ПП18, ПП26	Практичне заняття 7	5,5*	Тестування, навчальна дискусія,вирішення практичних задач
	Лекція 6		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 8		Проведення модульного контролю

Рекомендовані джерела: 1–21			
	Самостійна робота		1. Система правового регулювання соціальних інформаційних відносин 2. Інформаційно-пошукові системи 3. Інформація з обмеженим доступом та її захист з точки зору права 4. Співвідношення права на інформацію і права власника інформації з обмеженим доступом 5. Всього за темою 1 6. Злочини, пов'язані з використанням комп'ютерів 7. Злочини, пов'язані з порушенням авторських і суміжних прав з використанням комп'ютерних даних і систем 8. Розроблення й оцінювання захищених систем 9. Загрози безпеці інформації 10. Класифікація атак 11. Системний підхід до захисту ІТЗ 12. Ідентифікація й аутентифікація, керування доступом 13. Місце і роль уразливостей у математичній моделі процесу захисту інформації з повним перекриттям загроз 14. Рівні захисту інформації 15. Реалізація ядра безпеки 16. Модель захисту інформації в межах держави 17. Модель MRDB з категоріями у складі міток безпеки 18. Модель СЗІ реляційних СУБД 19. Модель СЗІ MRDB 20. Модель СЗІ безпечної БД 21. Уявлення елементів матриці 22. Властивості матриці 23. Програма оцінки ефективності систем захисту інформації"Оцінка СЗІ" 24. Експертиза в галузі технічного захисту інформації

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп’ютерний клас для проведення лабораторних та практичних занять.
  - Програмне забезпечення. Windows XP, 8,10, Microsoft Office, Ultra Zip Password Cracker 1.00 та Advanced ZIP Password Recovery 2.2, Network Skanner, Kasperski, Total Security, Chrome, IE, Mozilla Firefox, Opera, Acronis Disk Director, SimPass.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2019.-276с

2. Голубенко О.Л. Політика інформаційної безпеки / О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ: Вид: СНІ ім. В.Даля, 2019. – 300 с.
3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2019. – 608 с.
4. Департамент спеціальних телекомунікаційних систем та захисту інформації служби безпеки України. Н а к а з N 53 від 30.11.99. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації.
5. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
6. Закон України. Про державну таємницю. (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93)
7. Закон України. Про електронні документи та електронний документообіг. (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275).
8. Закон України. Про захист інформації в автоматизованих системах. (Відомості Верховної Ради (ВВР), 1994, N 31, ст.286).
9. Закон України. Про захист інформації в інформаційно-телекомунікаційних системах. Закон введено в дію з дня опублікування - 2 серпня 1994 року (згідно з Постановою Верховної Ради України.
10. Закон України. Про Національну систему конфіденційного зв'язку. (Відомості Верховної Ради України (ВВР), 2002, № 15, ст.103).
11. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л.: монографія “Базова модель експертної системи оцінки безпеки інформації в комп‘ютерних системах органів внутрішніх справ України” (шифр “Торсіон-1”). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту “Торсіон-1”. – К.: Видавництво НАВСУ, 2003. – 316с.
12. Ленков С.В. Методы и средства защиты информации. В 2-х томах. Том 1. Несанкционированное получение информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко; под ред. В.А. Хорошко. – К.: Арий, 2018. – 464 с., ил.
13. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2018. – 223 с
14. Наказ від 04.07.2008 N 112. Адміністрація державної служби спеціального зв'язку та захисту інформації України. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
15. НД ТЗІ 3.7-003 -2005 СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. Затверджено наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 8 листопада 2005 р. № 125. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
16. Перелік відомостей, що становлять службову інформацію і яким присвоюється гриф «Для службового користування» Затверджено 03.09.2022. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України.
17. Постанова Кабінет міністрів України від 29 березня 2006 р. N 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
18. Стандарт ISO/1EC 15408:2000. Information technology − Security techniques -Evaluation criteria for IT security.
19. Стандарт ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.
20. Указ президента України №56/2022. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»
21. Шорошев В.В. Основи формування політики безпеки комп’ютерних систем: наукове видання. – К.: Бізнес і безпека, 2016. – 141с.

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 (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «Правове забезпечення та системи захисту інформації обмеженого доступу»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «Уразливості та моделі захисту інформації обмеженого доступу»»	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 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-	**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 вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що	Відмінно / Зараховано (А)

	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.	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)
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 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*
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*

		окреслює мета та завдання дисципліни	*книжку не проставляється*